

NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS

WIRELESS LAN EXTENSION

by

Chye Bin Tay

March 2003

Thesis Advisor:
Second Reader:

Norman F. Schneidewind
Douglas E. Brinkley

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 2003	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Wireless LAN Extension			5. FUNDING NUMBERS	
6. AUTHOR(S) Chye Bin Tay				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) <p>The proliferation of laptop computers within the organization combined with increasing need to mobilize the labor force have fuelled the demand for wireless networks. Until recently, wireless technology was a patchwork of incompatible systems from a variety of vendors. The technology was slow, expensive and used for mobile applications or environments where cabling was impractical or impossible. With the maturing of industry standards and the deployment of lightweight wireless networking hardware across a broad market section, wireless technology has come of age. Lowered prices and interoperability have attracted many organizations to the idea, especially in the retail, financial, education, and health-care fields.</p> <p>The availability of wireless networking and wireless Local Area Networks (LANs) can extend the freedom and mobility of a network user, solve various problems associated with hard-wired networks and even reduce network deployment costs in some cases.</p> <p>This thesis provides an introduction to wireless LAN technology and the wireless LAN design for the Software Metrics Laboratory in Ingersoll 158, with particular emphasis on the communication requirements and protocols for the implementation of the wireless LAN extension to the existing wired LAN.</p>				
14. SUBJECT TERMS Wireless Local Area Networks, WIFI (802.11b), Access Point			15. NUMBER OF PAGES 85	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

WIRELESS LAN EXTENSION

Chye Bin Tay

Lieutenant Colonel, Republic of Singapore Air Force

B.Eng., University of Manchester Institute of Science & Technology, UK, 1990

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
March 2003**

Author: Chye Bin Tay

Approved by: Norman F. Schneidewind
Thesis Advisor

Douglas E. Brinkley
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The proliferation of laptop computers within the organization combined with increasing need to mobilize the labor force have fuelled the demand for wireless networks. Until recently, wireless technology was a patchwork of incompatible systems from a variety of vendors. The technology was slow, expensive and used for mobile applications or environments where cabling was impractical or impossible. With the maturing of industry standards and the deployment of lightweight wireless networking hardware across a broad market section, wireless technology has come of age. Lowered prices and interoperability have attracted many organizations to the idea, especially in the retail, financial, education, and health-care fields.

The availability of wireless networking and wireless Local Area Networks (LANs) can extend the freedom and mobility of a network user, solve various problems associated with hard-wired networks and even reduce network deployment costs in some cases.

This thesis provides an introduction to wireless LAN technology and the wireless LAN design for the Software Metrics Laboratory in Ingersoll 158, with particular emphasis on the communication requirements and protocols for the implementation of the wireless LAN extension to the existing wired LAN.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	REQUIREMENTS STATEMENT.....	1
B.	MOTIVATION.....	1
C.	CHALLENGES.....	3
	1. Security.....	3
	2. Interference.....	4
	3. Limited Power and Bandwidth.....	4
	4. Range.....	4
D.	THESIS ORGANIZATION.....	5
II.	BACKGROUND.....	7
A.	WIRELESS LAN TECHNOLOGY.....	7
	1. Narrowband Technology.....	7
	2. Spread Spectrum Technology.....	7
	a. <i>Frequency-Hopping Spread Spectrum Technology.....</i>	<i>8</i>
	b. <i>Direct-Sequence Spread Spectrum Technology.....</i>	<i>8</i>
	3. Infrared Technology.....	8
B.	NETWORK TOPOLOGY.....	10
	1. Wired Topology.....	10
	2. Wireless Topology.....	10
	a. <i>Peer-to-Peer Network.....</i>	<i>11</i>
	b. <i>Infrastructure Network.....</i>	<i>11</i>
	c. <i>Roaming.....</i>	<i>12</i>
	d. <i>Use of Directional Antennas.....</i>	<i>13</i>
C.	PHYSICAL MEDIA.....	14
D.	IEEE 802.11 WIRELESS STANDARD.....	15
	1. 802.11 Architecture.....	17
	2. IEEE 802.11 Services.....	18
	3. Carrier Sense Multiple Access-Collision Avoidance Mechanism.....	20
	a. <i>The RTS/CTS Mechanism.....</i>	<i>20</i>
	b. <i>Acknowledging the Data.....</i>	<i>21</i>
	4. Comparison of 802.11 Standards.....	21
III.	WIRELESS LAN DESIGN.....	25
A.	OVERVIEW.....	25
B.	SPECIFIC REQUIREMENTS.....	26
	1. Users Specifications.....	26
	a. <i>Type of Users.....</i>	<i>26</i>
	b. <i>Composition of Users.....</i>	<i>26</i>
	c. <i>Usage Rates.....</i>	<i>27</i>
	d. <i>User Applications.....</i>	<i>27</i>
	2. Hardware Specifications.....	28
	a. <i>Number of Laptop Computers.....</i>	<i>28</i>

	<i>b.</i>	<i>Number of Servers.....</i>	<i>28</i>
	<i>c.</i>	<i>Network Equipment.....</i>	<i>28</i>
	<i>d.</i>	<i>Number of Access Points</i>	<i>28</i>
	<i>e.</i>	<i>Backbone Needs</i>	<i>28</i>
3.		Software Specifications.....	30
	<i>a.</i>	<i>Workstation Operating System</i>	<i>30</i>
	<i>b.</i>	<i>Server Operating System.....</i>	<i>30</i>
	<i>c.</i>	<i>Network Protocols</i>	<i>30</i>
	<i>d.</i>	<i>IP Address and Names of Nodes.....</i>	<i>30</i>
	<i>e.</i>	<i>Subnet Address and Mask.....</i>	<i>30</i>
	<i>f.</i>	<i>Domain Servers</i>	<i>30</i>
4.		LAN Technology.....	31
	<i>a.</i>	<i>Type of Media</i>	<i>31</i>
	<i>b.</i>	<i>Speed of Media</i>	<i>31</i>
C.		NETWORK DIAGRAM.....	31
D.		LIST OF HARDWARE/SOFTWARE AND COST	33
	1.	Hardware	33
	2.	Software.....	34
	3.	Total Cost	34
E.		LABORATORY SITE LAYOUT	35
F.		SECURITY	36
	1.	Change the Default Network Name (SSID)	37
	2.	Disable the SSID Broadcast in the AP Beacon	37
	3.	Enabled Wired Equivalent Privacy (WEP)	37
	4.	Change Encryption Keys Periodically.....	38
	5.	Enable MAC Filtering on APs	38
IV.		CONCLUSION AND RECOMMENDATION	39
	A.	CONCLUSION.....	39
	B.	FUTURE WORK	39
	1.	Critical Issue of Operational Support	39
		<i>a.</i> <i>Implementing Wireless LAN Support Tools.....</i>	<i>40</i>
		<i>b.</i> <i>Monitoring the Network.....</i>	<i>40</i>
		<i>c.</i> <i>Configuration Management.....</i>	<i>40</i>
	2.	Beyond WEP.....	41
		<i>a.</i> <i>Virtual Private Network</i>	<i>41</i>
		<i>b.</i> <i>IEEE 802.1x</i>	<i>41</i>
		APPENDIX A CISCO AIRONET 1200 SERIES ACCESS POINT	45
		APPENDIX B ORINOCO 802.11A/B COMBO SPECIFICATIONS.....	57
		APPENDIX C SECURITY GUIDELINES FOR WIRELESS LAN.....	59
		LIST OF REFERENCES	67
		INITIAL DISTRIBUTION LIST	69

LIST OF FIGURES

Figure 1.	Wired LAN Topology	10
Figure 2.	A Wireless Peer-to-Peer or Ad-hoc Network.....	11
Figure 3.	Client and Access Point or Infrastructure Wireless LAN	12
Figure 4.	Multiple Access Points and Roaming	13
Figure 5.	The Use of Directional Antennas	14
Figure 6.	Wireless Protocol Stack	15
Figure 7.	802.11 Frame Format	17
Figure 8.	802.11 Architecture	18
Figure 9.	NPS Backbone.....	29
Figure 10.	SML158 Wireless and Wired LAN Network.....	31
Figure 11.	SML Wireless LAN Design Architecture	32
Figure 12.	SML Site Layout	35
Figure 13.	802.1x Authentication Process.....	43
Figure 14.	Orinoco 802.11a/b Combo Specifications	57
Figure 15.	Use of Firewall to Segregate Wireless LAN from Wired Network	62

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Comparison of Wireless LAN Technologies	9
Table 2.	IEEE 802.11 Terminology	16
Table 3.	IEEE 802.11 Services.....	19
Table 4.	Comparison of Wireless LAN Standards - 802.11a versus 802.11b.....	23
Table 5.	List of Hardware.....	33
Table 6.	List of Network Software.....	34
Table 7.	Summary of Cost.....	35
Table 8.	Summary of the Key Security Mechanisms That Can Be Implemented in a Wireless LAN.....	38

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The author would like to acknowledge the efforts of a number of individuals who have one way or another provided insight, guidance and motivation from the beginning to the completion of my thesis work. This thesis recognizes Professor Norman Schneidewind and Professor Douglas Brinkley for their patience and guidance during the research and completion of this thesis. I would also like to express my appreciation to the faculty and staff at the Naval Postgraduate School for their superb efforts to provide a first-rate education to all those fortunate enough to attend. Finally, I want to acknowledge the support, love and motivation of my wife, Margaret Chin Siew Hoong, and our two kids: son, Justin Tay Yee Wei, and daughter, Kristen Tay Yee Shen. They have been the author's true source of inspiration and happiness. Thank you all!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. REQUIREMENTS STATEMENT

A wireless LAN is a flexible data communications system implemented as an extension to, or as an alternative for, a wired LAN. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Thus, wireless LANs combine data connectivity with user mobility. These benefits extend the freedom of a network user, solve numerous problems associated with hard-wired networks and even reduce network deployment costs in some cases.

Wireless LANs were infrequently used until relatively recently. The reasons for this were high prices, low data rates, occupational safety concerns, and licensing requirements. Recent improvements in RF technology data rates combined with the falling deployment costs have made wireless LANs a more popular alternative to traditional wired LAN solutions. In fact, it has grown to be an essential education requirement in any academic institution.

This thesis provides an introduction to wireless LAN technology with particular attention to the wireless LAN design considerations. The main objective of this thesis is to create a wireless LAN design for the Software Metrics Laboratory (SML) in Ingersoll Hall, (room 158), in Naval Postgraduate School (NPS). The intention of the wireless LAN is to supplement the existing wired LAN in the SML. As NPS computer network classes constantly use the laboratory for teaching and research purposes, it is essential that the SML is equipped with both wired and wireless LAN capabilities.

B. MOTIVATION

Wireless LANs have gained popularity in a number of vertical markets, including the health-care, retail, manufacturing, warehousing, and even academia. These industries seem to have profited from the productivity gains of using hand-held terminals and laptops to transmit real-time information to centralized hosts for processing. Today, wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers. For example, public wireless LAN services are set to take off soon in Singapore and key countries in the Asia-Pacific region.

Despite being a small market, Singapore already has several service providers - from large telecom companies to small niche players - which offer 'hot spot' services. Hot spots are in public places such as hotels, airports, shopping malls and so on, and allow notebook computers and personal digital assistants (PDAs) to connect to a corporate network or send e-mail on the Internet. The user only needs to have a wireless LAN card to access this service.

The widespread reliance on networking in business and the rapid growth of Internet and online services are strong testimonies to the benefits of shared data and shared resources. Wireless LANs may offer the following productivity, convenience, and cost advantages over traditional wired networks:

- **Mobility**
Wireless LAN systems can provide LAN users with access to real-time information in their organizations even when they are on the move.
- **Installation Speed and Simplicity**
Installing a wireless LAN system eliminates the need to pull cable through walls and ceilings.
- **Installation Flexibility**
Wireless technology provides better installation flexibility than the wired systems.

Wireless LANs often augment rather than replace wired LAN networks. Essentially, it aims to provide the final few meters of connectivity between a wired network and the mobile user. The following list describes some of the many applications made possible through the flexibility of wireless LANs:

- Consulting or accounting audit teams or small workgroups increase productivity with quick network setup.
- Network managers in dynamic environments minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.
- Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

- Installing networked computers in older buildings with wireless LANs are a cost-effective network infrastructure solution.
- Trade show and branch office workers minimize setup requirements by installing pre-configured wireless LANs needing no local MIS support.
- Warehouse workers use wireless LANs to exchange information with central databases, thereby increasing productivity.
- Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.
- Senior executives in meetings make quicker decisions because they have real-time information at their fingertips.

C. CHALLENGES

Despite the benefits of wireless over wired LANs, the use of a wireless LAN to replace wired LANs has not happened to any great extent. The motivation to do so was not strong. These could be explained as follows: First, as LAN awareness became more significant, extensive pre-wiring for data applications were already factored into the design of new buildings; Second, there is an increasing reliance on twisted pair cabling for LANs and in particular, Category 3 and Category 5 unshielded twisted pair.

However, in a number of environments, there is a role for wireless LAN as an alternative to a wired LAN. Wireless LANs are applicable in areas where either adequate twisted pair connections are in short supply or new wiring is not allowed. Wireless LANs also have applications where it is no longer economical to install and maintain wired LANs. In most of these cases, an organization will also have wired LAN to support servers and some stationary workstations. This is an example of a LAN extension.

It is important to understand the constraints and limitations of Wireless LANs, as not everything new is good and foolproof. Today, there are a few important challenges facing wireless LAN design and implementation which are as follows:

1. Security

Wireless LAN communications are not private channels. Thus, anyone can access the public domain channel. There are security implications. They are easily susceptible to hackers trying to access sensitive information or spoil the operation of the network. It is easier to do a Denial of Service (DOS) attack for wireless than wired systems. A

mischievous person can use a wireless client to insert bogus packets into the wireless LAN with the intent of keeping users from getting access to services.

2. Interference

Also, since it is a public channel, it is difficult to manage the access and thus the potential is present for users to interfere with each other. The unlicensed nature of the radio-based wireless LANs means that other products transmitting in the same frequency spectrum can potentially interfere with the wireless network.

3. Limited Power and Bandwidth

Both power and bandwidth are limiting factors in mobile computing. All mobile devices such as laptops, PDAs, etc. depend on the internal battery for their power. The power will run out eventually unless it is continuously being charged. However, this is not a problem for wired systems, which do not depend on batteries for their power requirements. Another constraint facing wireless computing is the limited bandwidth with maximum of 54 Mbps¹. The current wireless technology is still not mature enough to accord the same level of bandwidth as the wired systems.

4. Range

The distance over which RF and Infrared (IR) waves can communicate is a function of product design (in transmitted power and receiver design) and the propagation path, especially in indoor environment. Building structures like walls, metal framework, and even people, can affect the manner in which energy propagates, and thus interfere with the range and coverage a particular system achieves. Most wireless LAN systems use RF waves because radio waves can penetrate most indoor walls and obstacles. However, the current range for typical wireless LAN systems varies from under 100 feet to more than 300 feet [Ref. 1].

Flexibility and mobility make wireless LANs both effective extensions and an attractive alternative to wired networks. Wireless LANs provide all the functionality of the wired LANs, without the physical constraints of the wire itself. However, the current wireless technology is still evolving and there are many challenges one needs to consider before implementing it. Given all these developments, it is imperative that computer network related classes taught in the SML keep up with the wireless technology.

¹ Wireless standards 802.11b and 802.11a/g provide up to 11 Mbps and 54 Mbps respectively.

D. THESIS ORGANIZATION

The thesis is organized as follows: Chapter II introduces the background on wireless LAN technology focusing on network topology, the physical media used, and provides an overview of the IEEE 802.11 wireless standard and explains its services. Chapter III discusses the design considerations and presents the design for the SML, which includes the user requirements, hardware specifications, software specifications and the estimated costing required. Finally, Chapter IV concludes the thesis and primarily discusses future work and areas of further research regarding wireless LAN design paralleling the research presented in this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. WIRELESS LAN TECHNOLOGY

Wireless technology is the method of delivering data from one point to another without using physical wires. The technology includes the radio and infrared spectrum and is employed by both terrestrial and satellite networks. Wireless LANs predominantly use radio waves as the physical media for transferring data. Manufacturers of wireless LANs have a range of technologies to choose from when designing a wireless LAN solution. Each technology comes with its own set of advantages and limitations. Current wireless LAN products fall into one of the following categories. [Ref.1]

1. Narrowband Technology

A narrowband radio system transmits and receives user information on a specific radio frequency. Narrowband radio strives to keep the radio signal frequency as narrow as possible and the bandwidth is just wide enough to pass the information. Carefully coordinating different users on different channel frequencies prevents undesirable crosstalk between communications channels.

A good illustration of the narrowband concept is a private telephone line. When each home in a neighborhood has its own private telephone line, people in one home cannot listen to calls made to other homes. In a radio system, we achieve privacy and noninterference by using discrete radio frequencies. The radio receiver filters out all radio signals except the ones on its designated frequency. However, one drawback of narrowband technology is that the end-user or customer must obtain an FCC license for each employed site. This is something we would not want for the SML wireless LAN design, as it would be costly.

2. Spread Spectrum Technology

Spread spectrum was developed during World War II to provide security for military radio communications. It spreads a signal across a wide range of frequencies at very low power, transforming the original signal into a noise-like signal. This hides the signal and makes it difficult for the signal to be detected. In fact, spread spectrum was designed to be resistant to noise, interference, jamming and unauthorized detection, making this technology ideal for wireless networking. Most wireless LAN systems use

spread-spectrum technology. Spread-spectrum technology is comprised of two competing technologies-Frequency Hopping (FHSS) or Direct Spread Spectrum Technology DSSS).

a. Frequency-Hopping Spread Spectrum Technology

FHSS uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.

b. Direct-Sequence Spread Spectrum Technology

DSSS functions by dividing the data into several pieces and simultaneously sending the pieces on as many different frequencies as possible, unlike FHSS, which sends on a limited number of frequencies. This process allows for greater transmission rates than FHSS, but is vulnerable to greater occurrences of interference. This is because the data is spanning a larger portion of the spectrum at any given time than FHSS. In essence, DHSS floods the spectrum all at one time, whereas FHSS selectively transmits over certain frequencies.

3. Infrared Technology

A third technology, utilizes the infrared spectrum to transmit and receive digital data. IR systems have not seen widespread commercial adoption. Like light, IR cannot penetrate opaque objects and employs either directed (line-of-sight) or diffused technology. High performance directed IR systems are not practical for mobile users and thus are only used to implement fixed sub-networks. Diffused (or reflective) IR wireless LAN systems do not require line-of-sight, but the cells are limited to individual rooms. The range of inexpensive directed technology is limited (3ft) and thus typically used for personal area networks [Ref. 1]. As such, IR technology will not be suitable for the SML because of its short range.

Table 1 summarizes some of the key characteristics of these three technologies.

The DSSS and FHSS spread spectrum techniques have their pros and cons and the IEEE 802.11b standard supports both of them. Both DSSS and FHSS make it hard for anyone to intentionally or unintentionally intercept or jam the radio transmissions in a wireless LAN. To someone who does not have the correct frequency information, spread spectrum transmissions look no different from static or background noise. It is therefore

difficult to “wiretap” a wireless LAN and directly observe the raw data being carried in the network. Likewise, it is difficult to jam a spread spectrum transmission. To do that without knowing the correct frequency information, you will need to generate a signal that is strong enough to jam the entire frequency band.

	Infrared		Spread Spectrum		Narrowband
	Diffused Infrared	Directed Infrared	Frequency Hopping	Direct Sequence	Microwave
Data Rate	1 to 4	1 to 10	1 to 3	2 to 20	10 to 20
Mobility	Stationary/ mobile	Stationary with LOS	Mobile	Stationary/mobile	
Range (m)	15 to 60	25	30 to 100	30 to 250	10 to 40
Detect ability	Negligible		Little		Some
Wavelength/ frequency	λ : 800 to 900 nm		902 to 928 MHz 2.4 to 2.4835 GHz 5.725 to 5.85 GHz		902 to 928 MHz 5.2 to 5.775 GHz 5.275 to 5.8 GHz
Modulation Technique	ASK		FSK	QPSK	FS/QPSK
Radiated power	-		<1W		25mW
Access method	CSMA	Token Ring, CSMA	CSMA		Reservation ALOHA, CSMA
License required	No		No		Yes unless ISM

Table 1. Comparison of Wireless LAN Technologies
(From: William Stallings, “Wireless Communications and Networks, pp 441)

In comparison, FHSS is more secure and is therefore used more extensively in the military. This is because the carrier frequency used in DSSS is fixed and the security provided by the DSSS chipping code is limited. However, DSSS has better bandwidth (currently from 2 Mbps up to 11 Mbps) and range and is much more resilient to interferences than FHSS. DSSS is therefore more widely implemented in commercial wireless LAN products. And this wireless technology will be used for the SML wireless LAN design.

B. NETWORK TOPOLOGY

1. Wired Topology

Traditional LANs link Personal Computers (PCs), file servers, printers, and other network equipment using cables or optical fibers as the transmission medium as shown in Figure 1. Users communicate through the LAN, exchange electronic mail and access multi-user programs and shared databases.

To connect to the LAN, a user must plug a computer into the network wall or floor LAN outlet. This physical connection creates an environment of more or less stationary workstations. Moving from one location to another necessitates disconnecting from the LAN and reconnecting at the new site. Expanding a LAN usually means additional cabling, which can be time consuming and adds to the LAN's overhead. Large complex LANs servicing many users located in different rooms or on different floors of a building, are usually subdivided into segments to facilitate management.

The SML is currently configured with a wired LAN topology similar to Figure 1 but with Ethernet switch and hub.

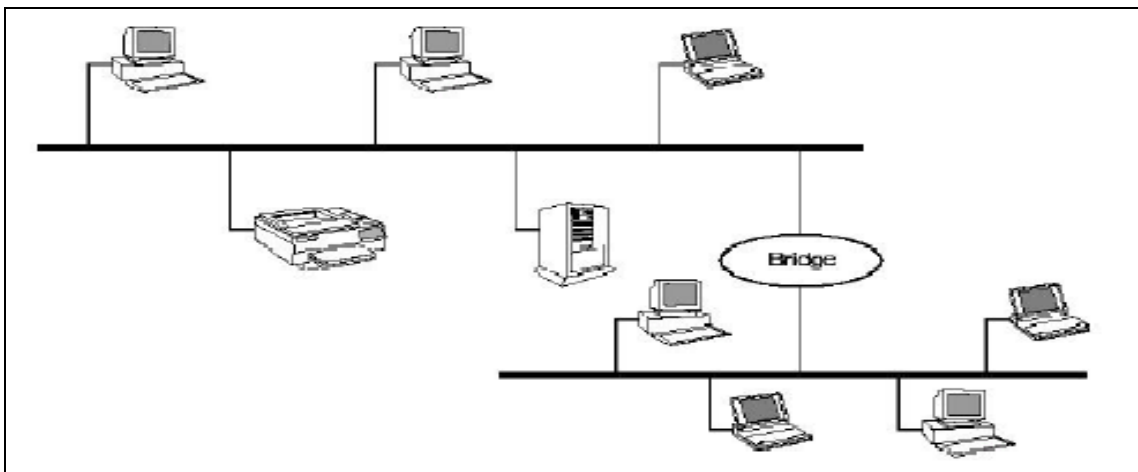


Figure 1. Wired LAN Topology
(From: www.alvarion-usa.com, Nov 02)

2. Wireless Topology

Wireless LANs allow workstations to access the network using radio propagation as the transmission medium. Adding a wireless Access Point (AP) to a wired LAN's switch or hub forms an LAN extension. While adaptable to both indoors and outdoors environments, wireless LANs are predominately used for indoor applications such as office buildings, manufacturing floors, hospitals, and universities. The basic building

block of the wireless LAN is the cell. This is the area in which the wireless communication can take place. The coverage area of a cell depends on the strength of the propagated radio signal and the type and construction of walls, partitions, and other physical characteristics of the indoor environment. PC-based workstations, notebook and pen-based computers can move freely in the cell and still remain connected to the network.

a. Peer-to-Peer Network

The network topology of Wireless LANs can be simple or complex. The simplest topology is a peer-to-peer or ad hoc network consisting of two or more PCs equipped with wireless adapter cards. These PCs can set up an independent network whenever they are within range of one another. Figure 2 illustrates a peer-to-peer or ad-hoc network. Peer-to-peer networks require no administration or pre-configuration. However, it is important to note that each client would only have access to the resources of the other client and not the services of a central server.

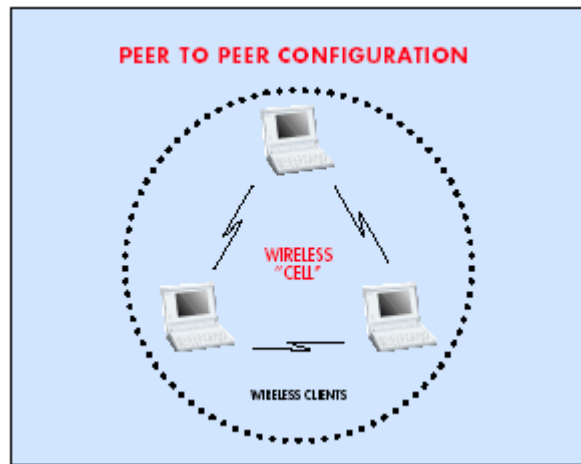


Figure 2. A Wireless Peer-to-Peer or Ad-hoc Network
(From: www.intermec.com, Jan 03)

Installing (AP) can extend the range of an ad-hoc network, effectively doubling the range at which the devices can communicate. The AP communicates with each wireless station in its coverage area. Stations also communicate with each other via the AP. Here, the AP functions as a relay, extending the range of the system.

b. Infrastructure Network

The AP also functions as a bridge between the wireless stations and the wired network. The AP can be connected to a hub or a switch on the wired network in

order to provide wireless services to a room or portion of a building. APs can also be used to wirelessly bridge two wired LAN segments or two wireless LAN segments. Cascading several wireless links, one after the other, can extend the range of the system. With the AP connected to the wired network, each client can access the server resources as well as to other clients. Figure 3 illustrates an infrastructure network. Each AP can accommodate many clients; the specific number depends on the number and nature of the transmissions involved.

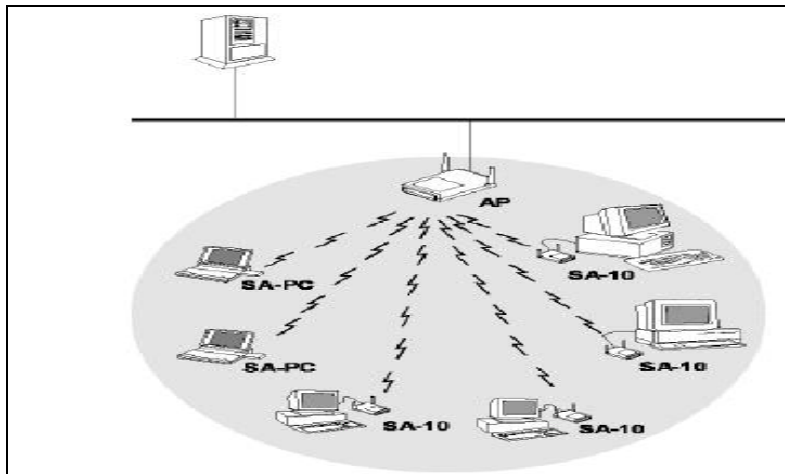


Figure 3. Client and Access Point or Infrastructure Wireless LAN
(From: www.alvarion-usa.com, Nov 02)

APs have a range, of 500 feet or 1000 feet for indoor and outdoor applications respectively. In a very large facility such as a warehouse or on a campus like NPS, it is probably necessary to install more than one AP. NPS has currently deployed about 30 APs around the campus [Ref. 6]. AP positioning is accomplished by means of a site survey. The goal is to provide a wireless coverage area by overlapping individual AP cells. By doing this, clients can roam throughout the coverage area without losing network contact. Each wireless station automatically establishes the best possible connection with one of the APs.

The infrastructure LAN topology would satisfy the wireless needs of SML since all the wireless clients would need to access a central server through 1 or 2 APs depending on the area of coverage required and range of the AP.

c. Roaming

Overlapping coverage areas are an important attribute of the wireless LAN setup. It is what enables seamless roaming between different APs and the associated

cells. Roaming allows mobile users with portable stations to move freely from one cell to another while maintaining a network connection. Roaming is seamless; a work session continues while moving from one cell to another. Multiple APs can provide wireless coverage for an entire building or campus. Figure 4 illustrates the roaming process. When the coverage area of two or more APs overlap, the stations in the overlapping area can establish the best possible connection with one of the APs, continuously searching for the best AP. In order to minimize packet loss during switchover, the “old” and “new” APs communicate to coordinate the process. This roaming feature would need to be considered if more than 1 APs are installed inside the SML.

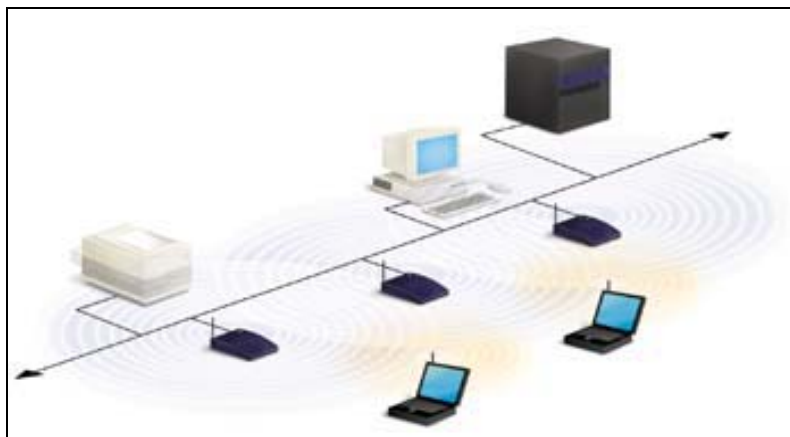


Figure 4. Multiple Access Points and Roaming
(From: www.proxim.com, Dec 02)

d. Use of Directional Antennas

Another important piece of wireless LAN equipment to consider is the directional antenna. Suppose we had a wireless LAN in building A and wanted to extend it to building B one mile away. One solution might be to install a directional antenna on each building each antenna targeting the other. The antenna on A connects to the wired network via an access point. The antenna on B similarly connects to an access point in that building, which enables wireless LAN connectivity in that facility. Figure 5 illustrates the use of directional antenna to bridge two separate wireless LANs.

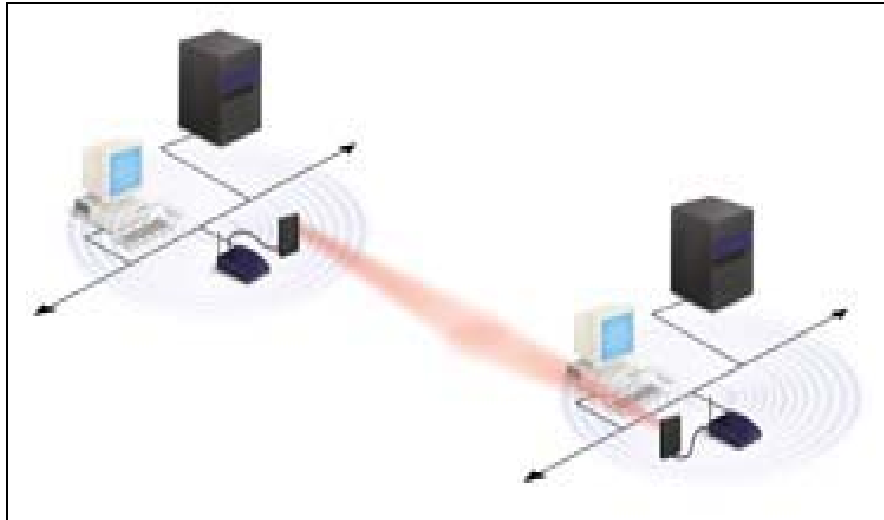


Figure 5. The Use of Directional Antennas
(From: www.proxim.com, Dec 02)

The use of directional antenna would not be necessary for the SML since it is located inside a small room and within the same building.

C. PHYSICAL MEDIA

[Ref. 2] Wireless LANs use electromagnetic airwaves (radio or infrared) to communicate information or data from one computer to another without relying on any physical connection. A network that uses electromagnetic radio waves is said to operate at radio frequency (RF), and the transmissions are referred to as RF transmissions. Each participating computer uses an antenna, which can transmit and receive RF. Physically; the antennas used within RF networks may be large or small, depending on the range desired. Radio waves are often termed as radio carriers because they perform the function of delivering energy to a remote receiver. To optimize the transmission of radio waves, and to be able to use them for communication purposes, the signal must be modulated, which is the process of boosting the signal into the RF range. This allows multiple signals to be transmitted simultaneously.

Multiple radio carriers can exist in the same space at the same time without interfering with each other provided that different transmitted radio frequencies are used. To extract data, a radio receiver tunes in one radio frequency while rejecting all other frequencies. Some inherent characteristics of RF waves need to be considered and remedied in the design of wireless networks, including signal-to-noise ratio, attenuation,

bouncing, refraction, and line of sight restrictions. These factors can be mitigated with careful engineering and with the appropriate placement of wireless equipment.

In a typical wireless LAN configuration, a transmitter/receiver (transceiver) device, which is the AP, connects to the wired network from a fixed location using standard Ethernet cabling. At a minimum, the AP receives, buffers, and transmits data between the wireless LAN and the wired network infrastructure. A single AP can support a small group of users and can function within a range of less than one hundred to several hundred feet. The AP (or the antenna attached to the AP) is usually mounted high but may be mounted essentially anywhere that is practical as long as the desired radio coverage is obtained.

End users access the wireless LAN through wireless-LAN adapters. These are PC cards that are inserted in notebook, palmtop, or desktop computers. Wireless LAN adapters provide an interface between the client network operating system (NOS) and the airwaves via an antenna. The nature of the wireless connection is transparent to the NOS. Figure 6 illustrates the wireless protocol stack.

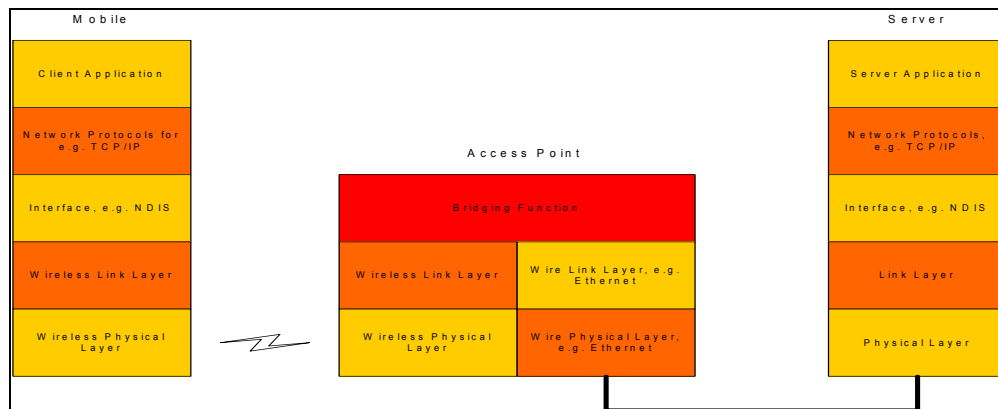


Figure 6. Wireless Protocol Stack

D. IEEE 802.11 WIRELESS STANDARD

Wireless data-networking vendors made equipment based on proprietary technology before the adoption of the 802.11 standard. Potential wireless customers were afraid of being 'locked in' with a specific vendor. They thus turned to more standards-based wired technology. The only possibility that wireless LANs would generally be accepted would be if the wireless hardware involved had a low cost and had become commodity items like routers and switches. Recognizing that the only way for this to

happen would be if there were a wireless data-networking standard, the Institute of Electrical and Electronics Engineers' (IEEE's) 802 Group undertook the challenge.

[Ref. 1] The IEEE 802.11 was finally released in 1997 after nearly seven years of development. Since that time, costs associated with deployment of an 802.11-based network have dropped, and wireless LANs has gained wide recognition and rapid deployment in schools, business and homes. Table 2 briefly defines key terms used in the IEEE 802.11 standard.

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within BSS is permitted to transmit and may be able to receive Protocol Data Units.
Distribution System (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the Logical Link Control layer (LLC) ² at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

Table 2. IEEE 802.11 Terminology
(After: William Stallings, "Wireless Communications and Networks, pp 457)

The standard specifies physical layer and medium access control (MAC) protocols. See Figure 7 that shows the 802.11 frame format. The MAC constitutes the lower half of the data link layer in the OSI network model. 802.11 were designed so that to upper levels the network behaves like a standard wired network. To accomplish this the link layer engages in error correcting functions that are not usually employed at the link layer in wired LANs.

² [1] In IEEE 802 protocol architecture, the LLC provides an interface to higher layers and performs flow and error control.

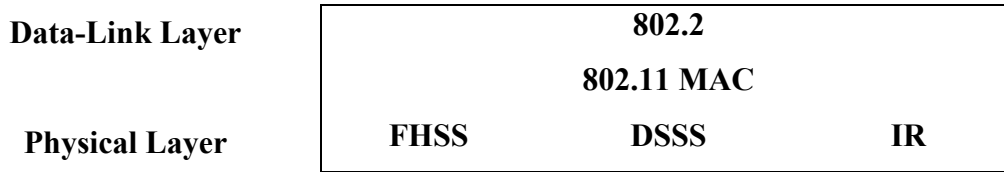


Figure 7. 802.11 Frame Format

At the physical layer, 802.11 specifies use of the 2.4-GHz Industrial, Scientific and Medical (ISM) band with both frequency-hopping and direct-sequence spread-spectrum at 1 Mbps with optional 2-Mbps throughputs. Power can range from 10 mW to 1 W. In trying to accommodate every possible variation in technology, the standard specifies an IR physical layer as well but very little development has occurred with it due to line-of-sight limitations. The majority of 802.11 implementations utilize the DSSS method.

At the data-link layer, 802.11 specifies a MAC protocol based on carrier-sense-multiple-access with collision avoidance and an optional request-to-send and clear-to-send mechanism that allows longer uninterrupted transmissions. The standard also provides for optional time-bounded services such as voice and video communications by allowing APs to control communications using polling methods.

1. 802.11 Architecture

[Ref. 1] Figure 8 illustrates the model developed by the IEEE 802.11 working group. The 802.11 architecture contains several main components: station (STA), access point (AP), independent basic service set (IBSS), basic service set (BSS), distribution system (DS), and extended service set (ESS). It is important to highlight these, as the wireless LAN design for the SML would essentially base on all these components. The wireless STA contains an adapter card, PC Card, or an embedded device to provide wireless connectivity. The AP functions as a bridge between the wireless STAs and the existing network backbone for network access.

An IBSS is a wireless network, comprising at least two STAs, used where access to a DS is unavailable. An IBSS is also sometimes regarded as an ad-hoc or peer-to-peer wireless network.

A BSS includes connectivity to the existing network backbone through an AP. A BSS is also sometimes referred to as an infrastructure wireless network. All STAs in a BSS communicate through the AP. The AP provides connectivity to the wired LAN and provides bridging functionality when one STA initiates communication to another STA.

An ESS consists of multiple BSSs interconnected by a DS. Typically, the DS is a wired backbone LAN (the NPS backbone LAN is a DS) but can be any communications network. ESS allows for mobility, because STAs can move from one BSS to another BSS. APs can be interconnected with or without wires; however, most of the time they are connected with wires. The DS is the logical component used to interconnect BSSs. The DS provides distribution services to allow for the roaming of STAs between BSSs. The ESS set-up in Figure 8 fits the wireless LAN design requirements for the SML.

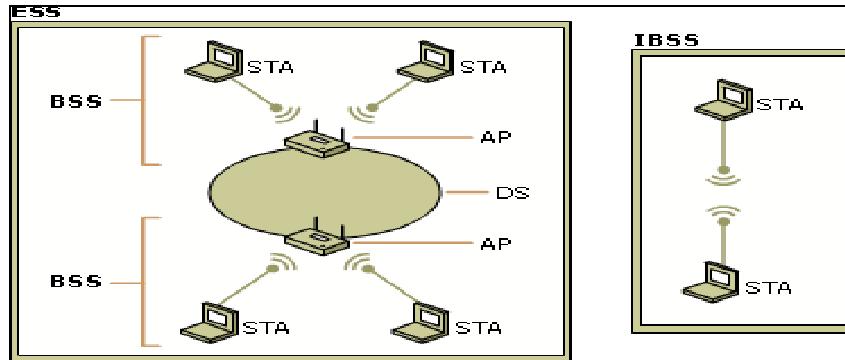


Figure 8. 802.11 Architecture
(From: www.microsoft.com, Jan 03)

2. IEEE 802.11 Services

[Ref. 1] There are in total nine services defined by IEEE 802.11 that need to be provided by the wireless LAN to provide adequate functionality similar to that which is inherent to wired LANs. Table 3 lists the nine services.

The service provider can be either the STA or the DS. Station services are implemented in every 802.11 station, which includes AP stations. Distribution services are provided between BSSs; these services may be implemented in an AP or in another special-purpose device attached to the DS. Three of the services are used to control IEEE 802.11 LAN access and confidentiality. The remaining six services are used to support delivery of the MSDUs between stations. The MSDU is a block of data delivered from the MAC user to the MAC layer; typically this is a LLC PDU.

Service	Provider	Used to Support	Functions
Association	Distribution system	MSDU delivery	Establishes an initial association between a STA and an AP within a particular BSS. The STA identity and address must be known before it can transmit or receives frames on a wireless LAN.
Authentication	Station	LAN access and security	Used to establish the identity of STAs to each other. IEEE 802.11 requires mutually acceptable, successful authentication before a STA can establish an association with an AP.
Deauthentication	Station	LAN access and security	This service is invoked whenever an existing authentication is to be terminated.
Disassociation	Distribution system	MSDU delivery	A notification from either a STA or an AP that an existing association is terminated. A STA should provide this notification before leaving an ESS or shutting down.
Distribution	Distribution system	MSDU delivery	Exchange MAC frames when the frame must traverse the DS to get from a STA in one BSS to a STA in another BSS.
Integration	Distribution system	MSDU delivery	Enables transfer of data between a STA on an IEEE 802.11 LAN and a STA on a wired LAN physically connected to the DS.
MSDU delivery	Station	MSDU delivery	Information that is delivered as a unit between MAC users.
Privacy	Station	LAN access and security	Used to prevent the contents of messages from being read by unauthorized users. The standard provides for the optional use of encryption to assure privacy.
Reassociation	Distribution system	MSDU delivery	Enables an established association to be transferred from one AP to another, allowing a mobile STA to move from one BSS to another.

Table 3. IEEE 802.11 Services

(After: William Stallings, “Wireless Communications and Networks, pp 459)

Wireless stations, when entering the range of an AP; choose a wireless AP to associate with. This selection is made automatically by using signal strength and packet error rate information. Next, the wireless station selects the assigned frequency of the AP that it is to begin communicating with. Periodically, the wireless station listens to other APs to determine whether they would provide a stronger signal or a better error rate. If a different AP provides a better signal, the workstation switches to the frequency of that AP. This process is called reassociation.

Reassociation can occur for many different reasons. The signal can weaken because the wireless station moves away from the AP or the AP becomes congested with too much other traffic or interference. The wireless station, by switching to another wireless station, can distribute the load over adjacent APs, increasing the performance of other wireless stations. By using a pattern of overlapping channels, coverage over large areas can be achieved. As a wireless station moves about, it can associate and reassociate from one AP to another, maintaining a continuous connection during transit. Thus, this is one key consideration for the SML design; it must ensure seamless connection as a mobile client associates and reassociates from one AP to another.

3. Carrier Sense Multiple Access-Collision Avoidance Mechanism

The basic access mechanism for 802.11 is carrier sense multiple access collision avoidance (CSMA-CA) with binary exponential back off. This is very similar to the CSMA-collision detection, which belongs to the standard 802.3 (Ethernet), but with a few major differences.

Unlike Ethernet, which sends out a signal until a collision is detected, CSMA-CA takes great care to not transmit unless it has the attention of the receiving unit, and no other unit is talking. This is called listening before talking (LBT). Before a packet is sent, the wireless device will listen to hear if any other device is transmitting. If the transmission is happening, the device will wait for a randomly determined period of time, and then listen again. The device will begin transmitting only if no one else is using the medium. Otherwise, it will wait again for a random time before listening once more. [Ref. 3]

a. The RTS/CTS Mechanism

To minimize the risk of the wireless device transmitting at the same time as another wireless device (and thus causing a collision), 802.11 employed a mechanism called Request To Send/Clear To Send (RTS/CTS). For example, if data arrived at the AP destined for a wireless node, the AP would send a RTS frame to the wireless node requesting a certain amount of time to deliver data to it. The wireless node would then respond with a CTS frame saying that it would stave off any other communications until the AP was done sending the data. Other wireless nodes would hear the transaction taking place, and delay their transmissions for that period of time as well. In this way, data is transmitted between nodes with a minimal likelihood that a collision would take place.

b. Acknowledging the Data

When sending the data across a radio signal with the inherent risk of interference, the chances that a packet will get lost between the transmitting radio and the destination unit are much greater than in a wired network system. Acknowledgement (ACK) was thus introduced to make sure that data transmissions would not get lost in the ether. The acknowledgement portion of CSMA-CA means that when a destination host receives a packet, it sends back a notification to the sending unit. If the sender does not receive an ACK, it will know that this packet was not received and will transmit it again. All this takes place at the MAC layer.

4. Comparison of 802.11 Standards

The maturity of wireless LAN technology based on the 802.11b standard, introduced in late 1999, has spawned a variety of reasonably priced wireless products. What's more, new 802.11a products are gaining momentum, as is the promise of a third standard, 802.11g.

Wireless devices adhering to the 802.11b standard actually work and, for most part, are interoperable, meaning that one manufacturer's AP will work with another's wireless PC card. Prices have fallen as well. Two years ago an AP cost about \$1,000; today we can buy one for as low as \$100 (Ref. www.ebay.com). The agency that tests for interoperability is an industry consortium known as the Wireless Ethernet Compatibility Alliance (WECA). Those 802.11b products that pass the WECA's tests are given the Wi-Fi (wireless fidelity) seal of approval. The IEEE 802.11b specification makes use of 2.4GHz band and has throughput of 11 Mbps. There are many different devices

competing for airspace in the 2.4GHz radio spectrum. Most of these devices are actually common household products like microwaves and cordless phones. Thus, the viability of an 802.11b network depends on how many of these products are near the network devices. So, if 802.11b were chosen as the wireless standard for SML, then one important consideration would be to ensure that these household products are not available anywhere near or inside the SML.

Today, the most common work performed across the wireless LANs entails office applications, such as e-mail, spreadsheet building, Web browsing, and word processing. Both 802.11b and 802.11a are adequate to handle such traffic. However, as streaming video and dynamic content become more common, the throughput of 802.11b products will not be enough.

This is where 802.11a comes in, a new specification that represents the next generation of enterprise-class wireless LANs. Because it operates in the 5GHz spectrum, it offers more bandwidth and thus more channels than 802.11b. 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM), a new encoding scheme that offers benefits over spread spectrum in channel availability and data rate. Channel availability is significant because the more independent channels that are available, the more scalable the wireless network becomes. The high data rate is achieved by combining many lower-speed sub-carriers to create one high-speed channel. 802.11a uses OFDM to define a total of 8 non-overlapping 20MHz channels; each of these channels is divided into 52 sub-carriers, each approximately 300KHz wide. In contrast, 802.11b uses only 3 non-overlapping channels.

	IEEE 802.11b	IEEE 802.11a
Time Table	Standard in 1997, Products in 2000	Standard in 2001, products in 2002
Frequency Band and bandwidth	Transmit at 2.4 GHz - IEEE 802.11g standard increases speed of 802.11b to 22 Mbps in the same 2.4 GHz band	5 GHz
Speed	11 Mbps (Effective speed - half of rated speed)	54 Mbps (Effective speed - 50% rated speed)
Modulation Technique	Spread Spectrum	OFDM (Orthogonal Frequency Division Multiplexing)
Distance Coverage	Up to 300 feet	60 feet - speed goes down with increased distance
Number of access points required	Every 200 feet in each direction	Every 50 feet;
Maturity	More matured products	Less matured but progressing fast
Market Penetration	Quite widespread	Just starting in 2002
Interference with other devices	Band is more polluted – significant interference here	Less interference because of few devices in this band
Interoperability	Not as problematic as 802.11a	Problems now but expect resolution soon
Cost	Cheaper - \$300 for access point and \$75 for adapter	More expensive \$ (500 in 01/2002 - will come down
Vendors	Major vendors in both camps	
No of Channels	3 non-overlapping channels	8 non-overlapping channels

Table 4. Comparison of Wireless LAN Standards - 802.11a versus 802.11b
(After: PC Magazine, May 21 2002)

While 802.11a and 802.11b use the same MAC layer technology, i.e. CSMA-CA, there are significant differences at the physical layer. 802.11b, using the ISM band, transmits in the 2.4GHz range, while 802.11a, using the Unlicensed National Information Infrastructure (U-NIL) band, transmits in the 5GHz range. Because their signals travel in different frequency bands, one significant benefit is that they will not interfere with each other. A related consequence, therefore, is that the two technologies are not compatible. Thus, 802.11a has some compatibility issues to work out as 802.11b products clearly dominate the market. Also, although all 802.11a products use the same chip set, their implementation by each manufacturer differs enough to make them incompatible. Until

interoperability standard is established, 802.11a products from one company may not talk with those of another.

As wireless technology is still relatively immature, there is tremendous potential for technology to change and grow. As such, the emphases for the wireless LAN design for the SML stressed on simplicity and scalability. For example, nearly all Wi-Fi networks worldwide use 802.11b standard. But it is not considered to be as secure or as fast as 802.11a, which is an approved standard that broadcasts a more powerful signal, running on 12 channels in 5GHZ spectrum, and transfers data up to five times faster than 802.11b. While it is faster, it has not been backward compatible to 802.11b, which is a problem. Another Wi-Fi standard known as 802.11g, which is more secure than 802.11b and has the speed of 802.11a, is in the works as well. However, the appropriate standards bodies have not approved it. More changes in the wireless standards arena are expected in near future.

In summary, the choice of the wireless LAN hardware and design for the SML should take into consideration these changes so as to avoid wastages. The criteria for vendor selection should contain these factors: a large market share, good recommendations from newsgroups, trade journals, and Subject Matter Experts, used by the military and universities, and must support 802.11a and b. About 50% of the NPS access points come from Cisco and using 801.11b. NPS wireless policy advocates the standardization of AP type from the same vendor [Ref. 6]. The rationale for this is to enhance the maintenance supportability, usability and security management.

III. WIRELESS LAN DESIGN

A. OVERVIEW

The goal of this chapter is to generate the requirements and design specification for a wireless LAN to supplement the existing wired LAN in the SML located in Ingersoll Hall, (room 158), at Naval Postgraduate School (NPS). In order to stay abreast of the latest advances in networking technologies, NPS computer network and software reliability classes, namely IS3502, IS3020 and SW4581³ require a laboratory that is equipped with both wired and wireless LAN capabilities. The primary objective of the SML laboratory is to provide the necessary technology support facilities to students attending any computer network classes conducted at NPS. It also serves to assist the staff and students in their research work and thesis projects specializing in network design. The laboratory resources are available for usage by any authorized staff and students at all times.

The goal of this research is to develop accurate user and stakeholder requirements and apply sound design principles to develop a wireless LAN solution for the SML. Aiding the process is the fact that wireless LAN's requirements are closely related to the same sort of requirements typical of any LAN. These requirements include high capacity, ability to cover short distances, full connectivity among the attached stations, and broadcast capability. The following list provides the principal considerations for the SML's wireless LAN design:

- **Simplicity.** Since it is intended to demonstrate the basic wireless LAN capability and features to NPS students undergoing the network classes, the design should be simple and not elaborate.
- **Minimize disruptions to existing wired LAN infrastructure.** The constraints of the project required the wireless design plan to make do with the existing wired laboratory infrastructure, space and electrical fittings as much as possible, and minimize disruptions to the current wired LAN configurations.

³ IS3020 is Software Design class. IS3502 is Computer Networks: Wide Area and Local Area class. SW4581 is Software Reliability class.

- **Connection to NPS backbone LAN.** Interconnection with stations on a wired backbone LAN is required. For infrastructure mode wireless LANs, this is usually accomplished through the use of control modules that connect to both the wired and wireless LANs.
- **Security.** The security considerations were established based on the existing NPS security guidelines and requirements for wireless LANs. The security for Internet connectivity is to be managed by the NPS network security administrator.
- **Service Area.** The wireless accessibility was to be confined within the laboratory. The laboratory has an area of 400 square feet. A typical coverage area for a wireless LAN has a diameter of 100 to 300m.
- **Handoff/roaming.** The AP configurations used in the wireless LAN should enable mobile stations to move from one cell to another within the laboratory.
- **License-free operation.** The design should be based on license-free operation, i.e. without the need to secure a license for the frequency band used by the LAN.
- **Scalability.** The choice of wireless hardware and design should be scalable as much as possible given the lack of wireless standards and the potential changes in wireless technology.

B. SPECIFIC REQUIREMENTS

1. Users Specifications

a. Type of Users

The users will consist of students enrolled in computer network and software reliability classes at NPS and also include staff and students involved in research.

b. Composition of Users

There are approximately 3 segments of computer network or software reliability classes offered each quarter. The students are primarily from the Computer Science, Software Engineering, and Information System Technology Curriculums.

c. Usage Rates

The instructor uses the laboratory approximately 10 hours a week. For the rest of the time, the lab will remain open for use by the students and faculty.

d. User Applications

The SML will primarily have Transmission Control Protocol/Internet Protocol (TCP/IP) applications, network design, monitoring, management application tools, software design, and software reliability programs installed and distributed throughout the LAN. Visio, Telnet, FTP, Traceroute and Ping are examples of the software and network applications employed by the SML.

Visio is a business graphic application that uses the concept of plastic drawing stencils to create drawings, and is thus very useful for network and software design and infrastructure drawing.

[Ref. 2] The Ping program sends a message to a remote computer and reports if the computer responds. The Traceroute program identifies intermediate computers along a path to a remote destination. Ping and Traceroute software is normally included in many operating systems.

Telnet is a terminal emulation program for TCP/IP networks such as the Internet. The Telnet client connects the PC to a server on the network. Users can then enter commands through the Telnet program and they will be executed as if the users were entering them directly on the server console. This enables users to control the server. To start a Telnet session, users must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

File Transfer Protocol, or FTP, is a protocol used to upload files from a workstation to a FTP server or download files from a FTP server to a workstation. It is the way that files get transferred from one device to another. FTP servers require the user to log on to the server in order to transfer files.

2. Hardware Specifications

a. Number of Laptop Computers

Ten shared laptops are required, as each laboratory section is comprised of approximately 20 students. Additionally, the laboratory has twenty desktops and available space is at a premium.

b. Number of Servers

One LAN server is required for application software and shared printing requirements. However, the existing wired LAN's server can be shared by the wireless LAN.

c. Network Equipment

The SML is already equipped with one 16-port Ethernet hub and one 16-port Ethernet switch. There are adequate ports left for the proposed 2 access points. Some Ethernet cables would be needed to connect the access points to the wired LAN and the ten laptops would also require ten radio Network Interface Cards (NIC). The NIC should all come from the same vendor.

d. Number of Access Points

The access point links the wireless users to the wired network of file servers and Internet access. Given the coverage of an access point using 802.11b standard, two access points (with radius of 300 feet) should be adequate to cover the 400 square feet laboratory area. The two access points could also act as redundancy for one another whenever one is down. As the wireless coverage area in SML is relatively small, no RF site survey is required. However, an accurate method to determine the number of required access points is to perform an RF site survey.

e. Backbone Needs

The NPS computer network is made up of a large number of small LAN's spread all over the campus. Thus, the NPS uses a fiber optic-cable as a transmission medium (backbone) that allows a higher bandwidth and lower delay to interconnect its main buildings to each other (intranet) and to facilitate their communications with the outside world via routers (internet). In addition, the NPS has installed Gigabit Ethernet network technology. The fiber optic-cable is directly linked to core Gigabit Ethernet

switches that are usually located on the first deck of each main building (network center). The data transmission speed of this switch is rated at 1Gbps, which utilizes the single mode fiber optics. Furthermore, within each deck in a main building, the core Gigabit Ethernet switch is connected to 3COM Ethernet switches (running at 155 Mbps) via multi mode fiber optic cable. Those switches are combined in two stacks. Each stack consists of four modules that manage a total of 96 ports. This patch panel is connected to each wall plate via Cat 5 that interconnects either individual workstations or hubs that form small LANs. Moreover, NPS uses many types of servers to support its educational and administrative functions. For instance, e-mail servers are dedicated to controlling incoming and outgoing mail messages while web-servers are employed to support the Internet and multipurpose servers are used to support NPS user accounts needs. Figure 9 shows NPS's backbone and network configuration.

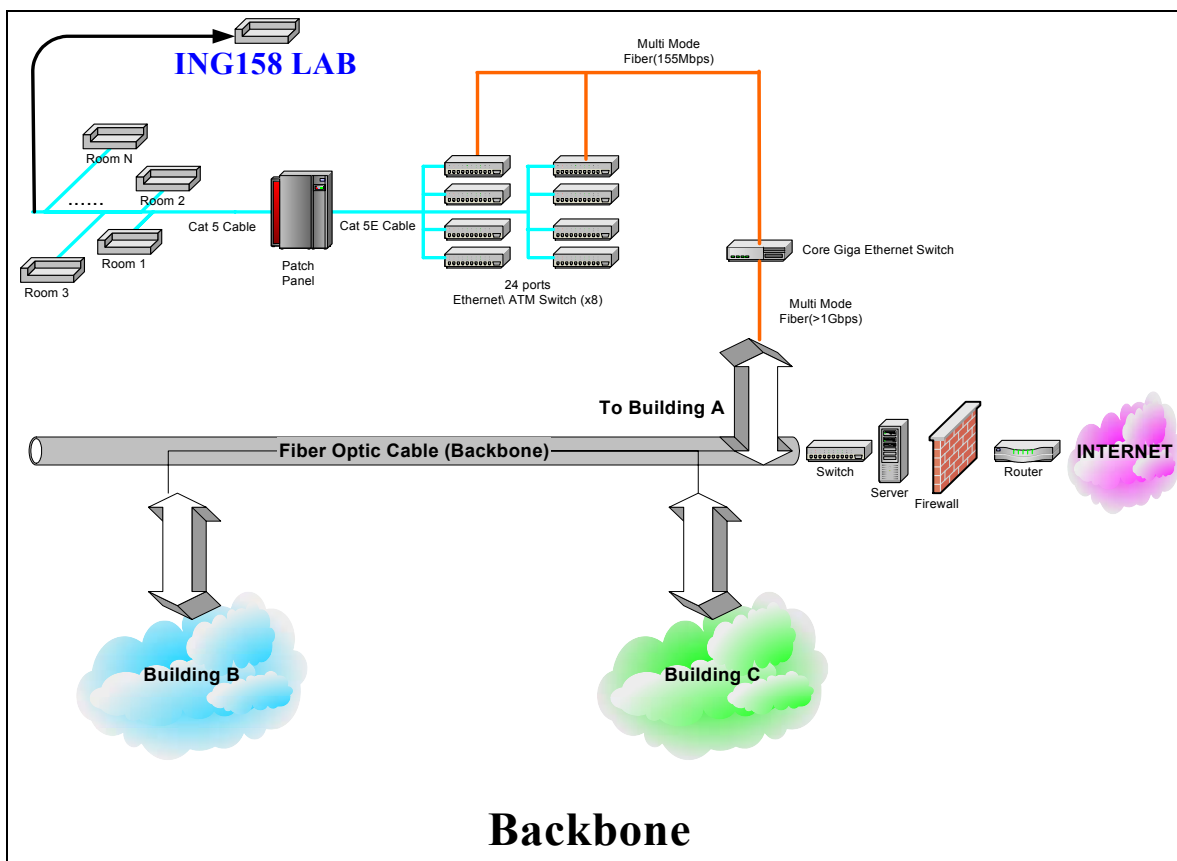


Figure 9. NPS Backbone

The NPS backbone requirements for the wireless LAN in SML is straightforward, as no additional hubs or switches would be purchased for the wireless

interfacing. The two Cisco APs will be connected to the existing Ethernet hub and switch, which belong to the wired LAN in the SML. The only requirement is to register the port numbers of the hub and switch intended for wireless connections with the NPS network administrator so that the SML wireless LAN could be legally established in NPS.

3. Software Specifications

a. Workstation Operating System

Microsoft XP

b. Server Operating System

Windows 2000 Server

c. Network Protocols

TCP/IP and Domain Name System (DNS). TCP/IP is a protocol suite used in the Internet to provide application programs with access to a connection-oriented communication service. DNS is an automated system used to translate computer names into equivalent IP addresses.

d. IP Address and Names of Nodes

IP Address (Server): 131.120.43.123

The existing wired LAN uses static IP addresses. The SML is using typical Class B IP addresses in a range from 131.120.43.111 to 131.120.43.254. Of these 254 addresses, only 21 (20 desktops and 1 server) of them are utilized. That leaves 233 addresses available to use between the APs and the laptops.

e. Subnet Address and Mask

Subnet Address: 131.120.43.x

The subnet address represents the ING158 SML location at NPS.

Subnet Mask: 255.255.252.0

The TCP/IP client ANDs the destination IP address with the subnet mask. If they are equal to 131.120.40.0, they belong to the same subnet and the packet remains in the subnet. If they are not equal, the destination IP address must be located in another subnet, i.e. the packet will be routed to its intended destination through the default router.

f. Domain Servers

DNS: 131.120.254.58 & 52

4. LAN Technology

a. *Type of Media*

Spread Spectrum using the ISM 2.4 GHz band for the wireless LAN. In addition, Ethernet Category 5 cables are used to connect the access points to the hub/switch and the hub/switch to the server.

b. *Speed of Media*

Up to 11Mbps for 802.11b standard and 100Mbps for Ethernet cables.

C. NETWORK DIAGRAM

The complete wireless and wired LAN set-up in the SML is given in Figure 10. The laboratory is divided into two compartments (Segment 1 and Segment 2). Segment 1, which is closer to the entrance, will be comprised of twelve workstations and five laptops, and Segment 2 will consist of eight workstations and five laptops.

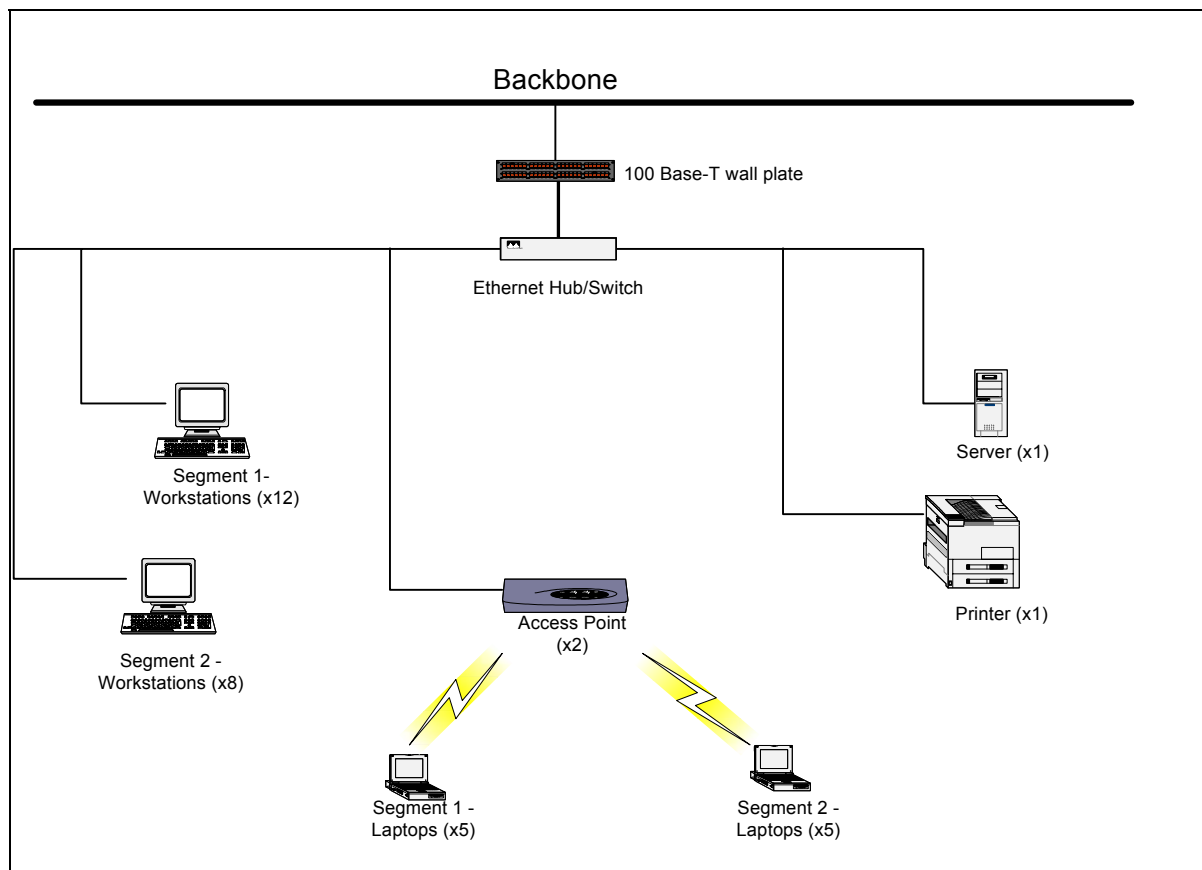


Figure 10. SML158 Wireless and Wired LAN Network

The second network diagram depicted in Figure 11 illustrates the wireless network architecture. Two Cisco Aironet 1200 Series APs are planned for the wireless

LAN design and should be adequate to provide continuous roaming within the SML. See Appendix A for the data sheet from Cisco on its AP. The Cisco Aironet 1200 Series protects current and future network infrastructure investments. The Aironet 1200 AP is able to do this through its compliance with both the IEEE 802.11a and 802.11b standards, and allows for both single- and dual-band configuration. Additionally these access points are field upgradable in order to modify these configurations as your requirements and technology evolve.

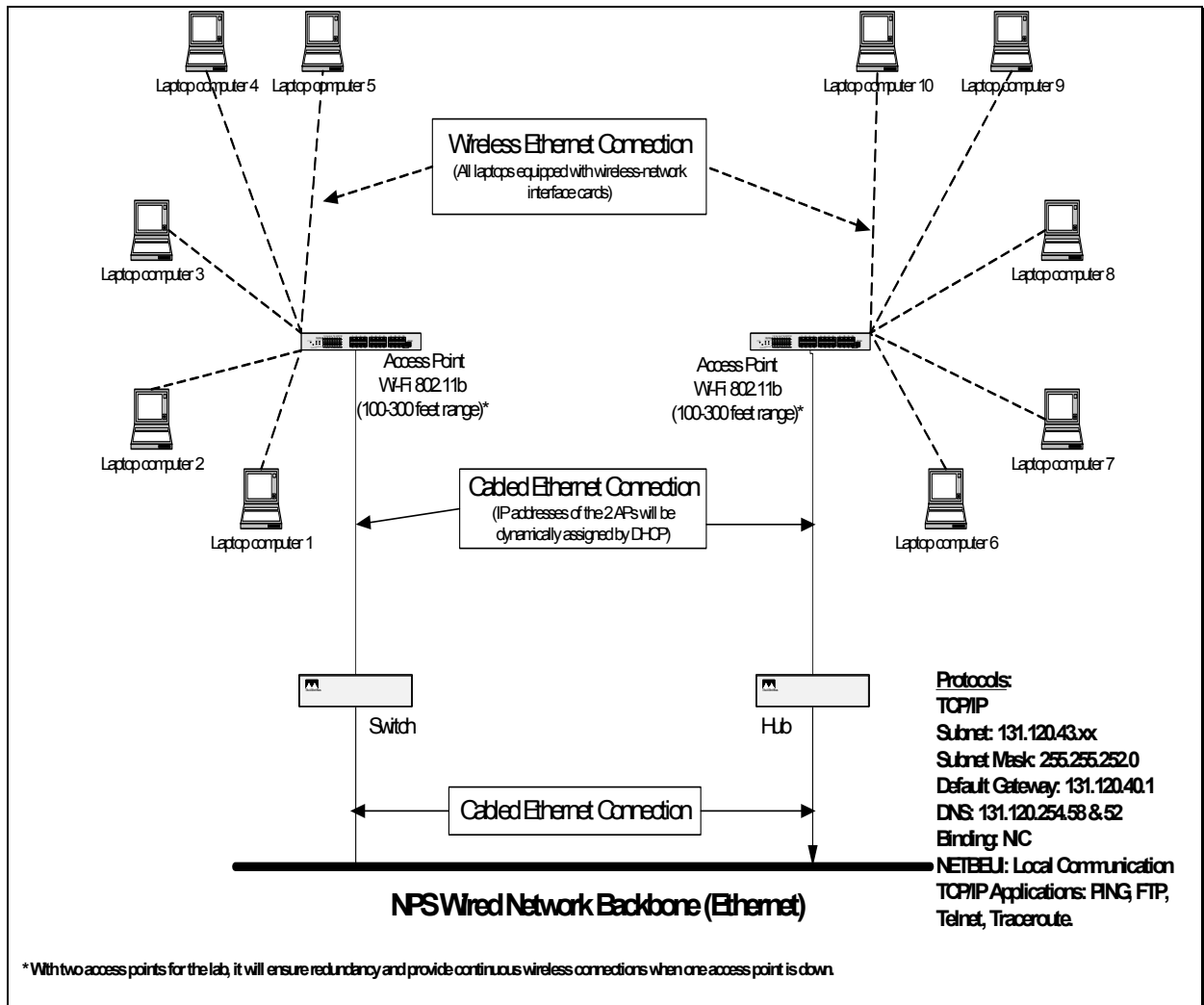


Figure 11. SML Wireless LAN Design Architecture

D. LIST OF HARDWARE/SOFTWARE AND COST

1. Hardware

Wireless LAN Hardware Equipment List					
Item	Specification	Qty	Cost	Subtotal	Justification
Laptops	Dell New Inspiron 2650 Mobile Intel® Pentium® 4 processors at 1.8GHz. 256MB. 30 GB hard drive. 14.1 XGA.	10	\$1299	\$12,990	The specifications were chosen based on network design and management requirements.
Access Point	Cisco Aironet 1200	2	\$1,200	\$2,400	Cisco's Aironet 1200 AP was chosen because it is faster has more memory and can be upgraded easily. The Aironet 1200 comes equipped to set up an 802.11b network, but it is built in a way to add radios for both the 802.11a and 802.11g standards. Those radios are sold separately, and if installed, the wireless access point will be able to operate all three networks at once. But it does not break down the barrier keeping 802.11a and 802.11b networks from interacting with each other. In addition, this AP was chosen because NPS wireless committee wants to standardize all APs installed in campus. This is to facilitate management and enhance security management.
Wireless NIC cards	Orinoco 802.11a/b combo card. 11Mbps.	10	\$160	\$1,600	This was recommended since it allows communication with both standards and also is more scalable. See Appendix B for the technical specifications.
Cable	25FT100BT CAT5E CABLRJ45M/R J45M	2	\$ 7	\$14	Standard Ethernet cable to connect each access point to the hub/switch and connect the hub to the server.
LAN Hardware Equipment Total				\$17,004	
Hardware Reference		Specification	www.dell.com www.cisco.com www.orinocowireless.com		
		Prices	www.dell.com GSA (DoD) Contract # GS-35F-4076D		

Table 5. List of Hardware

2. Software

Item	Qty	Cost	Subtotal	Justification
Microsoft Windows 2000 Server	1	Bundled with server		The preferred server operating system for NPS and provides the resources needed for managing the 30 PC's in the computer network lab.
Microsoft XP Professional	10	Bundled with workstations		The standard workstation operating system for desktop pc's at NPS. The ease of use and familiarity of the windows environment by the students and staff.
Microsoft Office 2000 Professional	10	Site licensed		The standard application for DOD. Offers ease of use and familiarity for basic applications needed by students to accomplish everyday schoolwork.
Adobe Acrobat Reader	10	Free Download		Gives students the ability to view and print Adobe PDF files.
Visual Studio 6.0 includes Microsoft Visual Basic®, Visual C++®, Visual J++®, and Visual FoxPro®	10	Site licensed		Software application development tool
Visible Analyst University Edition	10	Site licensed		Enables students to be able to do data modeling and application design
Visio 2000	10	Site licensed		A universal diagramming tool
Symantec Norton SystemWorks Professional 2002		\$89.99	\$89.99	For maintenance use by system administrator.
Norton Antivirus	10	Free with DON site license		One for each laptop.
Software Total			\$89.99	
Software References	Site Licenses	http://intranet.nps.navy.mil/code53/NPSSW/campsw.htm		
	Licensing	http://www.microsoft.com/		
	Specification	http://www.cnet.com/		
	Prices	http://www.microsoft.com/ http://www.staples.com/		

Table 6. List of Network Software

3. Total Cost

Thus, the total cost for the wireless LAN design proposal for the SML is \$18,183.99 (as summarized in Table 7).

S/No	Equipment	Cost
01	Hardware	\$17,004
02	Software	\$89.99
03	Chairs Adjustable (x 10 at \$109 each)	\$1,090
Grand Total		\$18,183.99

Table 7. Summary of Cost

E. LABORATORY SITE LAYOUT

The site layout is as shown in Figure 12. The diagram is not drawn to scale. The entire area of the laboratory is 400 square feet divided into two compartments of 200 square feet each.

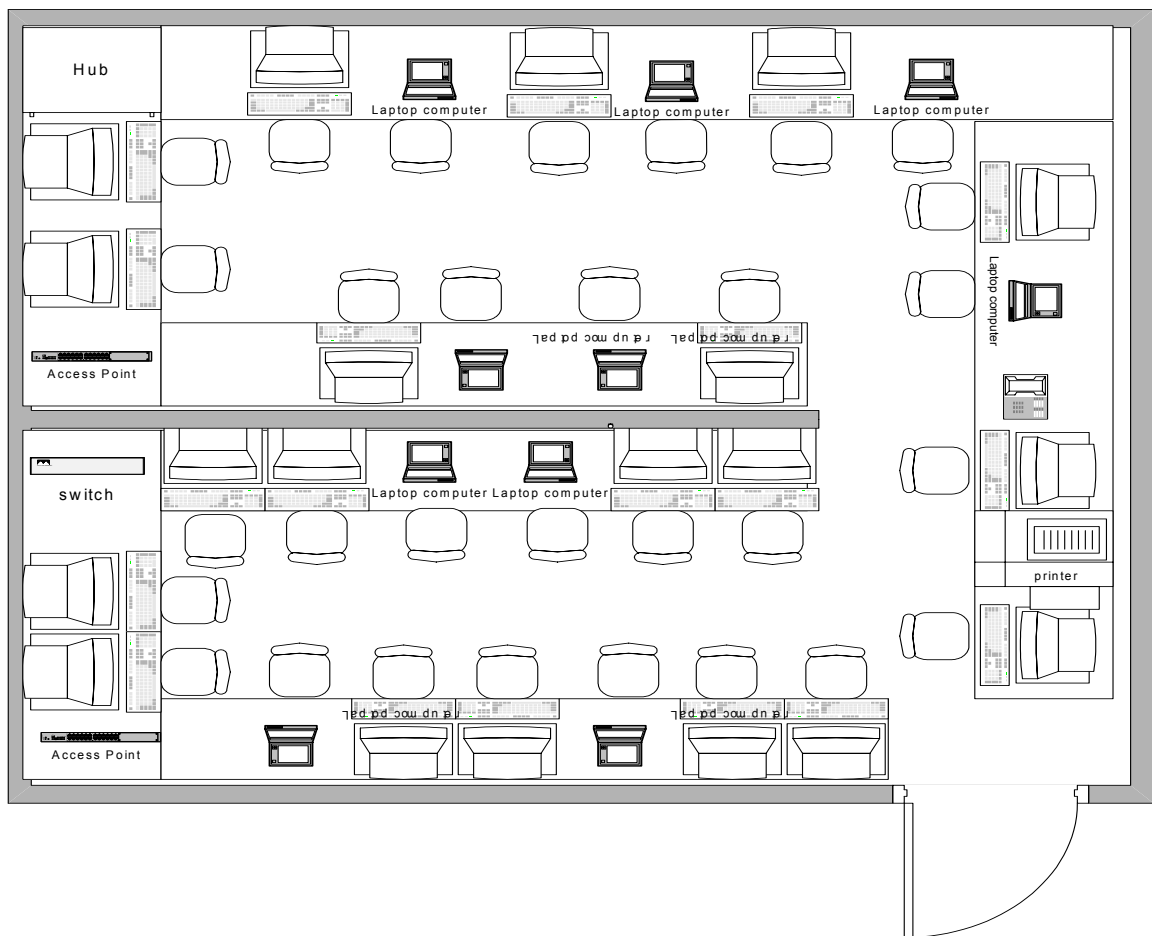


Figure 12. SML Site Layout

F. SECURITY

[Ref. 5] Security is by far the biggest challenge for a wireless LAN design and implementation, and undoubtedly warrants a separate thesis on it. With traditional wired LANs in the pre-Internet age, access to network is controlled by housing it within the office and hence logging on remotely was difficult. But with a wireless LAN, network communications are broadcast via radio waves past the office walls, through the building and can reach out into the car garage and beyond. Unless proper security is considered and implemented, anyone with the right tool and a little know-how can see the network traffic or gain access to the private network.

All wireless computer systems face security threats that can compromise its systems and services. Unlike the wired network, the intruder does not need physical access in order to pose the following security threats:

- **Eavesdropping.** This involves attacks against the confidentiality of the data that is being transmitted across the network. In the wireless network, eavesdropping is the most significant threat because the attacker can intercept the transmission over the air from a distance away from the premise of the company.
- **Tampering.** The attacker can modify the content of the intercepted packets from the wireless network and this results in a loss of data integrity.
- **Unauthorized access and spoofing.** The attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This kind of attack is known as spoofing. To overcome this attack, proper authentication and access control mechanisms need to be put up in the wireless network.
- **DOS.** In this attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. The attacker could also flood a receiving wireless station thereby forcing to use up its valuable battery power.

- **Other security threats.** The other threats come from the weakness in the network administration and vulnerabilities of the wireless LAN standards, e.g. the vulnerabilities of the Wired Equivalent Privacy (WEP), which is supported in the IEEE 802.11 wireless LAN standard.

For the SML wireless LAN design, it is recommended that the following security measures be implemented, at a minimum:

1. **Change the Default Network Name (SSID)**

SSID stands for **S**ervice **S**et **I**dentifier, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. The SSID differentiates one WLAN from another; so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network. An SSID is also referred to as a *Network Name* because essentially it is a name that identifies a wireless network. Hackers commonly know each manufacturer's default settings. As such, it is important to change the default SSID, which is needed to sign on to a WLAN and the default password on the AP.

2. **Disable the SSID Broadcast in the AP Beacon**

By default, APs periodically transmit their SSID values. Wireless utilities in Microsoft XP and freeware such as Network Stumbler⁴ capture this value and present a list of available networks to the user. Disabling this broadcast makes it more difficult for intruders to recognize the network.

3. **Enabled Wired Equivalent Privacy (WEP)**

Data is transmitted in readable form without encryption, and anyone within the radio range using a wireless protocol analyzer or a promiscuous-mode network adapter may capture the data without joining the network. WEP employs RC4 encryption, the same algorithm used for secure online shopping. WEP encryption can generally be found in 64-bit or 128-bit. Use the stronger 128-bit variety if available.

⁴ NetStumbler is a 802.11b tool that listens for available networks and records data about that access point.

4. Change Encryption Keys Periodically

The basic security rule applies, i.e. the less data transmitted with the same encryption key, the less vulnerable it will be.

5. Enable MAC Filtering on APs

Each wireless PC card has a unique identifier known as the MAC address. Many access points have the capability to build a list of MAC addresses that are permitted on the network. Those not listed are denied.

It is important to reiterate that the above steps are minimal; even if all the steps are taken, the data is still at risk. More stringent security considerations need to be put in place if the SML or NPS security requirements change. Table 8 summarizes how all the above security mechanisms work together to reduce the vulnerability of a wireless LAN against the specific threats of eavesdropping, tampering, unauthorized access, spoofing, and DOS. Appendix C provides more details on security guidelines for wireless LAN.

Protective Mechanism	Spread Spectrum	WEP Encryption	Wireless Network ID	Access	Network Authentication	Ethernet Address Restriction
Threat						
Eavesdropping	✓	✓				
Tampering	✓	✓				
Unauthorized Access & Spoofing		✓	✓		✓	✓
Denial of Service	✓					

Table 8. Summary of the Key Security Mechanisms That Can Be Implemented in a Wireless LAN.

IV. CONCLUSION AND RECOMMENDATION

A. CONCLUSION

Flexibility, ease, and mobility have certainly made wireless LAN attractive as a supplement to wired LAN. This by no means can justify wireless networks as complete replacement or substitute for wired networks. This is because wireless LAN still has some serious unresolved performance, security and standardization issues. At most, wireless LAN concept works well as a wired LAN extension especially in areas where drilling and wiring or cabling are no longer economical or practical.

Equipping the wireless LAN capability for the SML in Ingersoll Hall (Room 158) augurs well for its roles and functions as a teaching facility for NPS students undergoing computer network related classes. The design was meant to be simple and able to achieve its desired objectives. The laboratory will be able to demonstrate to the students not only its wired but also its wireless networking capabilities. Students would be able to make use of the network facilities for their course work and research.

Additionally, with so much development taking place with wireless LAN standards and technology, it is also important to design the SML wireless LAN with scalability in mind. The two Cisco Aironet 1200 series APs and the ten Orinoco 802.11a/b combo wireless cards were selected because they could be upgraded easily in the future and are able to utilize 802.11a, 802.11b and even 802.11g concurrently.

The biggest challenge facing wireless LANs today is their security inadequacies. Many would agree that it is not as secure as wired LANs. The popularity of wireless LANs will undoubtedly increase if the customers feel confident that they are secure and private. As such, improving the security for the wireless LAN design for the SML is an area for further research.

B. FUTURE WORK

1. Critical Issue of Operational Support

On any network, especially for wireless LANs, it is crucial to plan effective operational support to ensure that the network runs smoothly, because good operational support will enhance availability, performance, and security, and reduce costs. There is need for further research into supporting mechanisms for the wireless LAN in the

laboratory. To start, it is recommended that an operational support system for wireless LAN should consider the following:

a. Implementing Wireless LAN Support Tools

Support tools are needed so that network problems can be identified before they become serious. For example, the increase in packet retries on a particular AP could indicate RF interference in that area of the facility or collisions resulting from hidden nodes. The identification of a rogue AP can pinpoint a possible security threat. Support can identify and resolve these problems. Some wireless LAN support tools include products from AirWave, Symbol and Wavelink, which focus on the monitoring and configuration of APs and client devices. For example, the AirWave Management Platform is a comprehensive wireless network management solution that helps reduce support costs, improve network performance, and enforce security policies uniformly across the wireless LAN.

b. Monitoring the Network

The network is monitored for connectivity, status, availability, performance attributes and security settings. Monitoring needs to be done regularly by examining each AP and user. Again, tools like AirWave have features to indicate possible channel interference and environmental factors that impact performance. However, too much monitoring can have negative consequences as it introduces overhead on the network, which lowers throughput. As such, the network needs to be monitored sparingly. Most of the support tools have user-defined triggers that will automatically alert IT staff via a console, e-mail, or pager if problems crop up. For example, the software can trigger an alert if it detects an AP's configuration parameters are different from security policies, which may mean it is a rogue AP.

c. Configuration Management

The main benefit of some supporting tools is that they allow remote control of multi-vendor access points, and provide access to security settings, RF channel settings, SSID, power-over-Ethernet (PoE)⁵ control, and network management. The IT

⁵ A Power-over-Ethernet (PoE) or "Active Ethernet" solution only requires technicians to run one Ethernet cable to the access point for supplying both power and data. With PoE, power-sourcing equipment detects the presence of an appropriate "powered device" (e.g., an access point or Ethernet hub) and injects applicable current into the data cable. An access point can operate solely from the power it receives through the data cable. This allows greater flexibility in the locating of AP's and network devices and may significantly decrease installation costs.

staff uses a centralized console to perform configuration management of all APs instead of interfacing with each AP separately. Some support tools can even configure new APs automatically when they are found and ensure that they comply with security policies. This feature is good because the AP may be operating with factory default settings, which generally does not include any form of security. This ensures all APs are set the same, and thus improves security.

However, a sound operational support plan for wireless LANs is not inexpensive and one needs to weigh the pros and cons of the requirements versus the costs and manpower needs before deciding on the right balance.

2. Beyond WEP

Wireless provides convenience and mobility, but it also poses security challenges for network executives and security administrators. WEP is probably still adequate for most home use and the SML, depending on the confidentiality of the data. But in view of the major WEP vulnerabilities and security threats posed by wireless LANs, there is a need to identify better security to protect the SML wireless LAN. Described below are two current security techniques that can be researched further for a future thesis:

a. Virtual Private Network

When there is a need to transmit information via the wireless LAN, a further control measure, such as end-to-end encryption, should be used to ensure the confidentiality and integrity of the information, using a virtual private network (VPN) that runs over a wireless LAN. Another security feature of the VPN is that it allows authentication, which ensures that only authorized users can connect, send and receive information over the wireless LAN. A wireless LAN client transmits encrypted data through the AP to a VPN concentrator that decrypts the data and passes it onto the wired network. This solution can work well, particularly for small wireless LANs like SML, but may be too expensive and complex to implement for larger networks.

b. IEEE 802.1x

The problem is that there is no consensus for an open standard for wireless LAN security. Instead, there are proprietary wireless security methods, which require special client software and same-manufacturer APs and cards. This is not what the IEEE would want as the solution. A task group (TGi) was formed specifically to tighten up

wireless LAN security in a nonproprietary systematic format. [Ref. 7] The group has nearly completed a standard called Robust Security Network (RSN). This draft standard includes two parts: the Advanced Encryption Standard (AES)⁶ for encrypting wireless LAN traffic and the IEEE 802.1x Port-Based Network Authentication standard for wireless LAN user authentication and key management.

TGi proposed a stopgap measure called TKIP (Temporal Key Integrity Protocol), which is intended to work with existing and legacy hardware. These are products, which cannot support an upgrade to AES. TKIP uses a mechanism called fast-packet rekeying, which changes the encryption keys frequently. It provides better assurance than WEP but does not provide the same level of security achieved with AES. Because of this, IEEE does not recommend TKIP except as a patch to pre-RSN equipment [Ref. 8].

Current authentication in the 802.11 standard is focused more on wireless LAN connectivity than on verifying user or station identity. For enterprise wireless security to scale to hundreds or thousands of users, an authentication framework that supports centralized user authentication must replace the current method of authentication. TGi is working on 802.1x, an IEEE standard that provides an authentication framework for 802-based LANs. 802.1x will let wireless LANs scale by allowing centralized authentication of wireless users or stations. The standard is flexible enough to allow multiple authentication algorithms, and because it is an open standard, multiple vendors can innovate and offer enhancements.

In 802.1x, a wireless LAN user initiates an authorization request to the AP, which authenticates the client to an Extensible Authentication Protocol (EAP)-compliant Remote Authentication Dial-In User Service (RADIUS) server. This RADIUS server may authenticate either the user (via passwords) or machine (by MAC address). In theory, the wireless client is not permitted to join the network until the transaction is complete. Figure 14 illustrates the authentication process for 802.1x.

⁶ AES is a secure encryption cipher that is resistant to all currently known techniques of cryptanalysis. The US National Institute of Standards (NIST) has selected AES to replace the Data-Encryption Standard (DES and 3 DES) commonly used in VPN solutions.

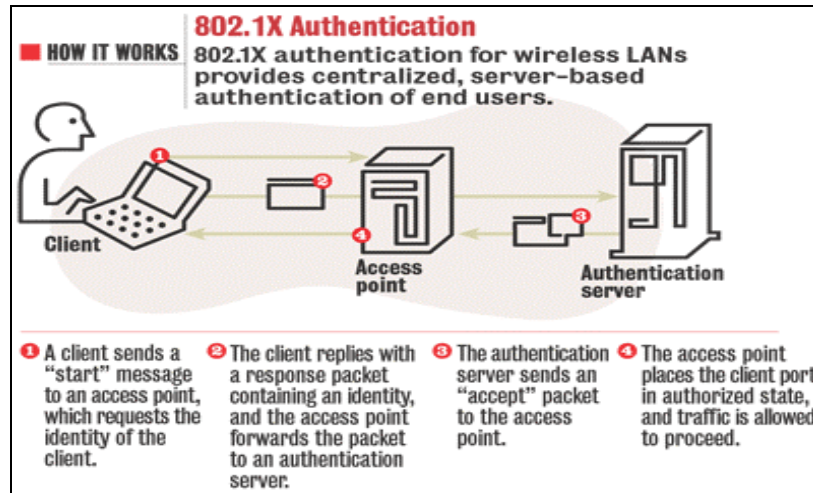


Figure 13. 802.1x Authentication Process
(From: <http://www.nwfusion.com/news/tech/2001/0924tech.html>)

In summary, there is need for future work for the SML wireless LAN. Building a reliable and highly available operational support mechanism, and enhancing the security implementation for the SML wireless LAN are two significant areas for further research. These areas are thus strongly recommended for thesis work in the next phase of the wireless LAN extension for SML.

THIS PAGE INTENTIONALLY LEFT BLANK

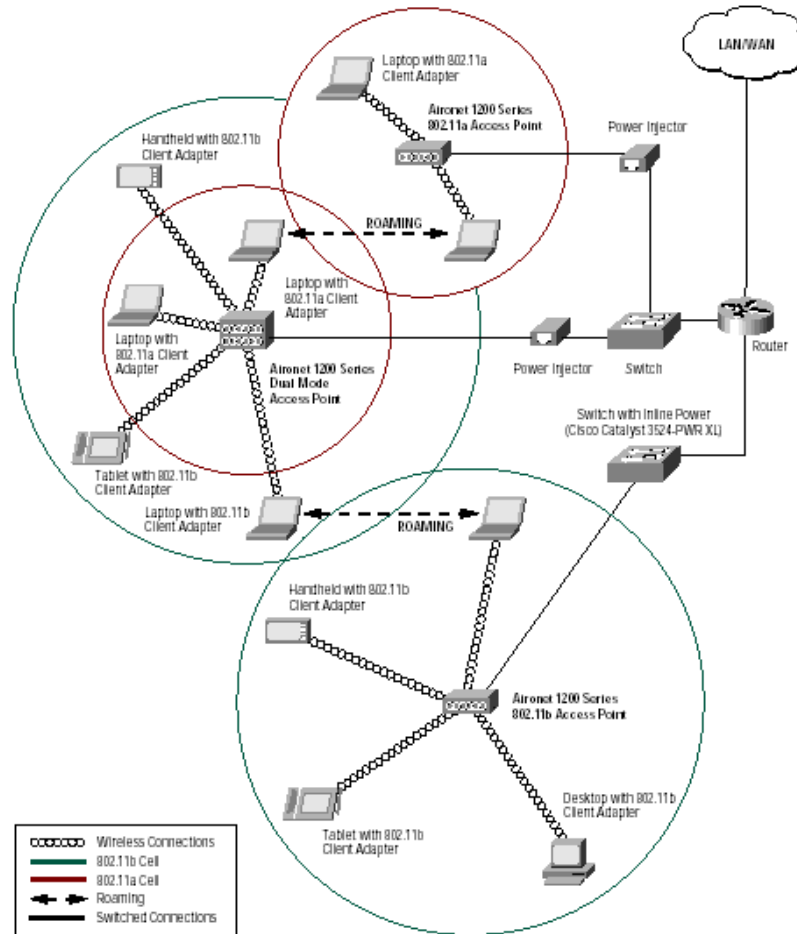
APPENDIX A CISCO AIRONET 1200 SERIES ACCESS POINT



PRODUCT OVERVIEW

[Ref. 4] The Cisco Aironet® 1200 Series AP sets the enterprise standard for next-generation high performance, secure, manageable, and reliable wireless local-area networks (WLANs), while also providing investment protection because of its upgrade capability and compatibility with current standards. The modular design of the Cisco Aironet 1200 AP supports IEEE 802.11a and 802.11b technologies in both single and dual-mode operation. You can configure the Cisco Aironet 1200 to meet customer-specific requirements at the time of purchase and then reconfigure and upgrade the product in the field as these requirements evolve. In addition, the Cisco Aironet 1200 Series creates a wireless infrastructure that provides customers with maximum mobility and flexibility, enabling constant connection to all network resources from virtually anywhere wireless access is deployed (Figure 1).

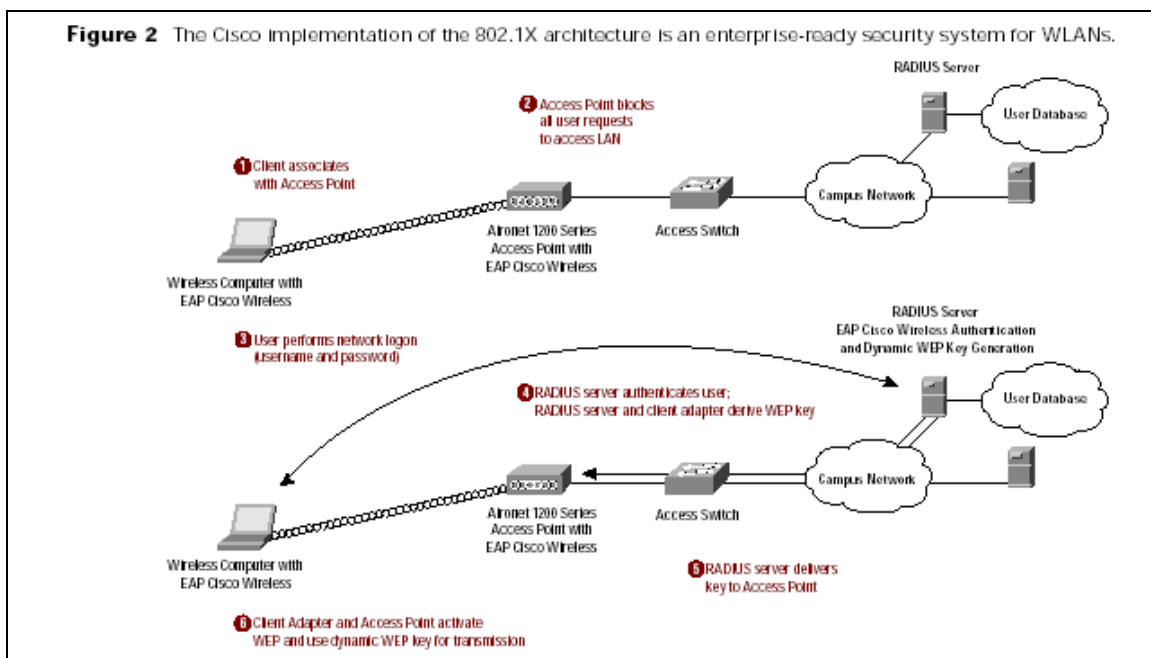
Figure 1 Configure the Cisco Aironet 1200 to support 802.11b, 802.11a, or both technologies in a single device. Legacy, current, and future clients can roam between access points while maintaining reliable and uninterrupted access to all network resources.



ENTERPRISE-CLASS SECURITY SOLUTION

Wireless LAN security is a primary concern. The Cisco Aironet 1200 Series addresses this issue with the award-winning Cisco-Wireless Security Suite, which is based on the IEEE 802.1X standard and its Extensible Authentication Protocol (EAP) to provide an enterprise-class solution (Figure 2). The Cisco Aironet 1200 Series supports all 802.1X authentication types, including EAP Cisco Wireless (LEAP), EAP-TLS, and types that take advantage of EAP-TLS. When coupled with a Remote Access Dial-In User Server (RADIUS) that supports the same authentication types, such as the Cisco Secure Access Control Server (ACS), the result is a scalable, centrally managed security solution that includes:

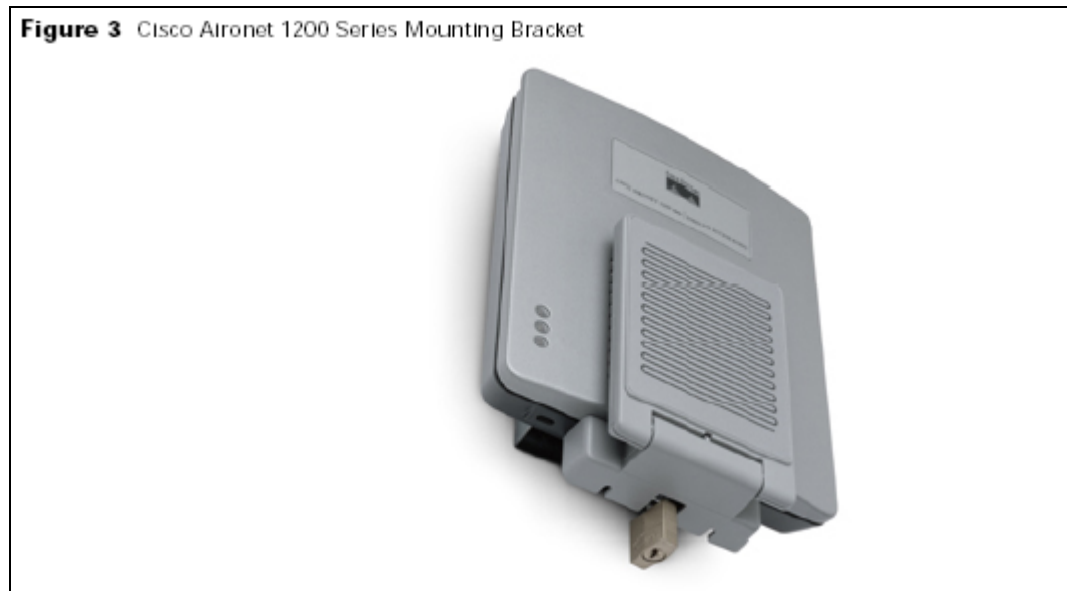
- Strong, mutual authentication to ensure that only legitimate clients associate with legitimate and authorized wireless access points
- Dynamic per-user, per-session encryption keys that automatically change on a configurable basis to protect the privacy of transmitted data
- Stronger WEP keys provided by pre-standard Temporal Key Integrity Protocol (TKIP) enhancements such as message integrity check (MIC) and per-packet keys via initialization vector hashing
- RADIUS accounting records for all authentication attempts



INVESTMENT PROTECTION FOR FUTURE-PROOF NETWORKS

With large storage capacity and support for Cisco management tools, the Cisco Aironet 1200 Series provides the capacity and the means to upgrade firmware and deliver new features as they become available. It features more than four times the amount of storage required by the initial firmware load and the tools for IS professionals to centrally and automatically upgrade firmware on often remote access points across the enterprise. For additional investment protection, the Cisco Aironet 1200 Series comes complete with an integrated mounting system that secures the device using the customer's choice of laptop security cables or standard padlocks (Figure 3). The reliability of the 2.4 GHz solution also makes the Cisco Aironet 1200 Series a wise investment.

It provides field-proven reliability, featuring a Cisco Aironet fourth-generation 802.11b radio. The 5 GHz radio maximizes capacity and performance, delivering up to 54 Mbps data rates on all eight available channels and allowing the wireless network to scale to accommodate a large number of users. With the Cisco Aironet 1200 Series, a single access point can add capacity to support new users by simultaneously operating one radio for high-speed 802.11a networked clients while maintaining another radio for 802.11b clients. The redundant hot-standby feature also aids in the overall reliability of the network by providing a backup access point in the rare case of a failure.



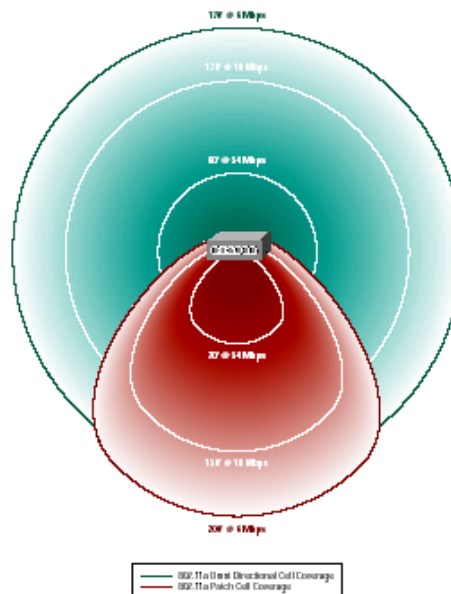
UNIQUE 802.11A 5 GHZ ANTENNA DESIGN FOR OPTIMAL COVERAGE

To extend the flexibility of deployments, the 802.11a radio module incorporates an articulating antenna paddle that contains both omni directional and patch antennas (Figure 4). For ceiling, desktop, or other horizontal installations, the omni directional antenna provides optimal coverage pattern and maximum range. For wall mount installations, the patch antenna provides a hemispherical coverage pattern that uniformly directs the radio energy from the wall and across the room (Figure 5). Both the omni directional and patch antennas provide diversity for maximum reliability even in high multipath environments such as offices and other indoor environments. Cisco provides this level of 5 GHz antenna flexibility and reliability to suit all installation scenarios.

Figure 4 The design of the 802.11a radio module features an integrated omni directional and patch antenna.



Figure 5 Cisco's innovative antenna module provides two distinct coverage patterns to address different access point installation orientations.



INTEGRATED MANAGEMENT TOOLS FOR RAPID CONFIGURATION

The Cisco Aironet 1200 Series simplifies wireless LAN management because many of the same management tools and capabilities available in wired networks are used on the wireless network (Figure 6). The 1200 Series supports network management through Simple Network Management Protocol (SNMP), Telnet, and a Web browser to aid in troubleshooting, monitoring, software download, and event logging. The CiscoWorks™ Wireless LAN Solution Engine is also available as a management tool. Table 1 provides product features and benefits, Table 2 provides product specifications, and Table 3 provides product system requirements for the Cisco Aironet 1200 Series.

Figure 6 The access point management system Express Setup screen provides all the settings required for basic configuration of the access point.

Home Map Help Uptime: 4 days, 21:55:10

System Name: AP1200
 MAC Address: 00:05:9a:38:42:70
 Serial Number: LLLYYWWXXXX

Configuration Server Protocol: DHCP
 Default IP Address: 192.168.129.20
 Default IP Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.129.235

AP Radio: Internal:
 Service Set ID (SSID): tsunami
 Role in Radio Network: Root Access Point
 Optimize Radio Network For: ☒ Throughput ☐ Range ☐ Custom
 Ensure Compatibility With: ☒ 2Mbit/sec Clients ☒ non-Aironet 802.11

AP Radio: Module:
 Service Set ID (SSID): tsunami
 Role in Radio Network: Root Access Point
 Optimize Radio Network For: ☒ Default ☐ Throughput ☐ Range ☐ Custom

Security Setup

SNMP Admin. Community:

Apply OK Cancel Restore Defaults

Table 1 Product Features and Benefits

Feature	Benefit
Modular platform for single or dual band operation	The access point can be configured for either 802.11b only, 802.11a only, or for simultaneous support of 802.11b and 802.11a to provide the maximum number of channels and maximum available data rates in a single device.
Field upgradable radios	Flexibility and investment protection is provided through field-upgradable card bus and mini-PCI radios. CardBus-based 802.11a modules can easily be fitted into installed Cisco Aironet 1200 Series access points.
5 GHz integrated antennas	Unique articulating antenna paddle incorporates high-gain omni directional and hemispherical patch antennas to deliver two distinct coverage patterns.
2.4- and 5 GHz Diversity Antennas	Diversity antennas for both the 2.4- and 5 GHz radios ensures optimum performance in high-multipath environments such as offices, warehouses, and other indoor installations.
Two reverse-polarity threaded naval connectors (RP-TNC) for external 2.4 GHz antenna connection	Diversity support for the 2.4 GHz radio to improve reliability in high-multipath environments. The RP-TNC connectors are compatible with the Cisco Aironet optional antennas, enabling WLAN architects to customize radio coverage for specific deployment scenarios.
Eight Mbytes Flash memory	Provides memory space for future firmware upgrades and supports new 802.11 standards and advanced features.
Support for Cisco Discovery Protocol and Software Image Manager (SWIM) within CiscoWorks Resource Essentials (RME)	Allows centralized and automatic firmware upgrades on remote access points across the enterprise.

Table 1 Product Features and Benefits (Continued)

Feature	Benefit
Standard 802.11b radio with 100-mW maximum transmit power and 85-dBm receive sensitivity at 11 Mbps data rate	2.4 GHz radio offers superior radio performance that results in industry-leading range. The greater the range of the access point, the fewer access points needed, resulting in lower total system cost.
802.11a radio module provides 40-mW maximum transmit power for UNII 1 and UNII2 bands and -68 dBm (typical) receive sensitivity at 54 Mbps data rate	Superior 5 GHz radio design provides industry-leading performance and receive sensitivity and maximum capacity through eight non-overlapping channels in the UNII1 and UNII 2 bands.
Support for both line power over Ethernet and local power (see Figures 7, 8, and 9)	To decrease the cost and complexity of installation, the Cisco Aironet 1200 Series can be powered over an Ethernet cable, eliminating the need to run expensive AC power to remote access-point installation locations. Depending upon radio configuration, the Cisco 1200 Series can be powered via Cisco line-power-enabled switches, multiport midspan power panels, or single-port power injectors. In instances where AC power is available at the installation location, the power supply for the Cisco Aironet 1200 Series can be plugged into an electrical outlet.
Aesthetically pleasing cast aluminum case, Underwriters Laboratories (UL) 2043 certification, and extended operating temperature (-20 to 55°C or -4 to 131°F)	The product design meets the aesthetic requirements of the enterprise and the rugged features support deployment in factories, warehouses, and the outdoors (in a NEMA enclosure). The broad operating temperature range and UL 2043 certification for plenum rating requirements set by local fire codes supports installation in environmental air spaces such as areas above suspended ceilings.
Multipurpose mounting bracket	Flexibility of the multipurpose mounting bracket gives numerous deployment options for site-specific requirements.
Two separate locking mechanisms for the access point and radio	Theft deterrence has become a requirement as wireless LANs proliferate into public areas. Additional investment protection is provided with built-in locking mechanisms.

Table 2 Product Specifications

	With 802.11a radio installed	With 802.11b radio installed	With both 802.11a and 802.11b radio installed
Part number	Configurable: AIR-AP1200 and AIR-RM20A-x-K9 (x=Regulatory Domain) Pre-Configured: • AIR-AP1220A-x-K9 • A=FCC • S=Singapore • T=Taiwan • J=TELEC (Japan) Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.	Configurable: • AIR-AP1200 and AIR-MP20B-x-K9 (x=Regulatory Domain) Pre-configured: • AIR-AP1220B-x-K9 • A=FCC • C=MII (China) • E=ETSI • I=Israel • J=TELEC (Japan) Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.	Configurable: • AIR-AP1200, AIR-RM20A-x-K9 and AIR-MP20B-x-K9 (x=Regulatory Domain) Pre-configured: • AIR-AP1220B-x-K9 and AIR-RM20A-x-K9 • A=FCC • C=MII (China) • E=ETSI • I=Israel • J=TELEC (Japan) • S=Singapore • T=Taiwan Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.
Radio module form factor	• CardBus (32-bit)	• Mini-PCI (32-bit)	• 802.11a: CardBus (32-bit) • 802.11b: Mini-PCI (32-bit)
Data rates supported	• 6, 9, 12, 18, 24, 36, 48, 54 Mbps	• 1, 2, 5.5, and 11 Mbps	• 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps • 802.11b: 1, 2, 5.5, and 11 Mbps

Table 2 Product Specifications (Continued)

	With 802.11a radio installed	With 802.11b radio installed	With both 802.11a and 802.11b radio installed
Network standard	<ul style="list-style-type: none"> IEEE 802.11a 	<ul style="list-style-type: none"> IEEE 802.11b 	<ul style="list-style-type: none"> IEEE 802.11a IEEE 802.11b
Uplink	<ul style="list-style-type: none"> Autosensing 802.3 10/100BASE-T Ethernet 	<ul style="list-style-type: none"> Autosensing 802.3 10/100BASE-T Ethernet 	<ul style="list-style-type: none"> Autosensing 802.3 10/100BASE-T Ethernet
Frequency band	<ul style="list-style-type: none"> 5.15 to 5.35 GHz (FCC UNII 1 and UNII 2) 5.15 to 5.25 GHz (TELEC) 5.15 to 5.25 GHz (Singapore) 5.25 to 5.35 GHz (Taiwan) 	<ul style="list-style-type: none"> 2.412 to 2.462 GHz (FCC) 2.412 to 2.472 GHz (ETSI) 2.412 to 2.484 GHz (TELEC) 2.412 to 2.462 GHz (MII) 2.422 to 2.452 GHz (Israel) 	<ul style="list-style-type: none"> 5.15 to 5.35 GHz (FCC UNII 1 and UNII 2) 5.15 to 5.25 GHz (TELEC) 5.15 to 5.25 GHz (Singapore) 5.25 to 5.35 GHz (Taiwan) 2.412 to 2.462 GHz (FCC) 2.412 to 2.472 GHz (ETSI) 2.412 to 2.484 GHz (TELEC) 2.412 to 2.462 GHz (MII) 2.422 to 2.452 GHz (Israel)
Network architecture type	<ul style="list-style-type: none"> Infrastructure, star topology 	<ul style="list-style-type: none"> Infrastructure, star topology 	<ul style="list-style-type: none"> Infrastructure, star topology
Wireless medium	<ul style="list-style-type: none"> Orthogonal Frequency Division Multiplexing (OFDM) 	<ul style="list-style-type: none"> Direct sequence spread spectrum (DSSS) 	<ul style="list-style-type: none"> 802.11a: Orthogonal Frequency Division Multiplexing (OFDM) 802.11b: Direct sequence spread spectrum (DSSS)
Media Access Protocol	<ul style="list-style-type: none"> Carrier sense multiple access with collision avoidance (CSMA/CA) 	<ul style="list-style-type: none"> Carrier sense multiple access with collision avoidance (CSMA/CA) 	<ul style="list-style-type: none"> Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation	<ul style="list-style-type: none"> (OFDM subcarrier) BPSK @ 6 and 9 Mbps QPSK @ 12 and 18 Mbps 16-QAM @ 24 and 36 Mbps 64-QAM @ 48 and 54 Mbps 	<ul style="list-style-type: none"> DBPSK @ 1 Mbps DQPSK @ 2 Mbps CCK @ 5.5 and 11 Mbps 	OFDM: <ul style="list-style-type: none"> BPSK @ 6 and 9 Mbps QPSK @ 12 and 18 Mbps 16-QAM @ 24 and 36 Mbps 64-QAM @ 48 and 54 Mbps DSSS: <ul style="list-style-type: none"> DBPSK @ 1 Mbps DQPSK @ 2 Mbps CCK @ 5.5 and 11 Mbps
Operating channels	<ul style="list-style-type: none"> FCC: 8 TELEC (Japan): 4 Singapore: 4 Taiwan: 4 	<ul style="list-style-type: none"> ETSI: 13; Israel: 7; North America: 11; TELEC (Japan): 14; MII: 11 	5 GHz Band: <ul style="list-style-type: none"> FCC: 8 TELEC (Japan): 4 Singapore: 4 Taiwan: 4 2.4 GHz Band: <ul style="list-style-type: none"> ETSI: 13; Israel: 7; North America: 11; TELEC (Japan): 14; MII: 11
Nonoverlapping channels	<ul style="list-style-type: none"> Eight (FCC only) Four (Japan, Singapore, Taiwan) 	<ul style="list-style-type: none"> Three 	<ul style="list-style-type: none"> Eleven

Table 2 Product Specifications (Continued)

	With 802.11a radio installed	With 802.11b radio installed	With both 802.11a and 802.11b radio installed
Receive sensitivity	<ul style="list-style-type: none"> • 6 Mbps: -85 dBm • 9 Mbps: -84 dBm • 12 Mbps: -82 dBm • 18 Mbps: -80 dBm • 24 Mbps: -77 dBm • 36 Mbps: -73 dBm • 48 Mbps: -69 dBm • 54 Mbps: -68 dBm 	<ul style="list-style-type: none"> • 1 Mbps: -94 dBm • 2 Mbps: -91 dBm • 5.5 Mbps: -89 dBm • 11 Mbps: -85 dBm 	<ul style="list-style-type: none"> • 1 Mbps: -94 dBm • 2 Mbps: -91 dBm • 5.5 Mbps: -89 dBm • 6 Mbps: -85 dBm • 9 Mbps: -84 dBm • 11 Mbps: -85 dBm • 12 Mbps: -82 dBm • 18 Mbps: -80 dBm • 24 Mbps: -77 dBm • 36 Mbps: -73 dBm • 48 Mbps: -69 dBm • 54 Mbps: -68 dBm
Available transmit power settings	<ul style="list-style-type: none"> • 40 mW (16 dBm) • 20 mW (13 dBm) • 10 mW (10 dBm) • 5 mW (7 dBm) <p>Maximum power setting will vary according to individual country regulations.</p>	<ul style="list-style-type: none"> • 100 mW (20 dBm) • 50 mW (17 dBm) • 30 mW (15 dBm) • 20 mW (13 dBm) • 5 mW (7 dBm) • 1 mW (0 dBm) <p>Maximum power setting will vary according to individual country regulations.</p>	<p>802.11a:</p> <ul style="list-style-type: none"> • 40 mW (16 dBm) • 20 mW (13 dBm) • 10 mW (10 dBm) • 5 mW (7 dBm) <p>802.11b:</p> <ul style="list-style-type: none"> • 100 mW (20 dBm) • 50 mW (17 dBm) • 30 mW (15 dBm) • 20 mW (13 dBm) • 5 mW (7 dBm) • 1 mW (0 dBm) <p>Maximum power setting will vary according to individual country regulations.</p>

Table 2 Product Specifications (Continued)

	With 802.11a radio installed	With 802.11b radio installed	With both 802.11a and 802.11b radio installed
Range (typical at maximum transmit power setting, 2.2 dBi gain diversity dipole antenna for 2.4 GHz; 6 dBi gain patch and 5 dBi omni antenna for 5 GHz)	<p>Omni directional Antenna:</p> <ul style="list-style-type: none"> • Indoor: <ul style="list-style-type: none"> – 60 ft (18m) @ 54 Mbps – 130 ft (40m) @ 18 Mbps – 170 ft (52m) @ 6 Mbps • Outdoor: <ul style="list-style-type: none"> – 100 ft (30m) @ 54 Mbps – 600 ft (183m) @ 18 Mbps – 1000 (304m) ft @ 6 Mbps <p>Patch Antenna:</p> <ul style="list-style-type: none"> • Indoor: <ul style="list-style-type: none"> – 70 ft (21m) @ 54 Mbps – 150 ft (45m) @ 18 Mbps – 200 ft (61m) @ 6 Mbps • Outdoor: <ul style="list-style-type: none"> – 120 ft (36m) @ 54 Mbps – 700 ft (213m) @ 18 Mbps – 1200 ft (355m) @ 6 Mbps 	<p>Indoor:</p> <ul style="list-style-type: none"> • 130 ft (40m) @ 11 Mbps • 350 ft (107m) @ 1 Mbps <p>Outdoor:</p> <ul style="list-style-type: none"> • 800 ft (244m) @ 11 Mbps • 2000 ft (610m) @ 1 Mbps 	<p>802.11a Omni directional Antenna:</p> <ul style="list-style-type: none"> • Indoor: <ul style="list-style-type: none"> – 60 ft (18m) @ 54 Mbps – 130 ft (40m) @ 18 Mbps – 170 ft (52m) @ 6 Mbps • Outdoor: <ul style="list-style-type: none"> – 100 ft (30m) @ 54 Mbps – 600 ft (183m) @ 18 Mbps – 1000 ft (304m) @ 6 Mbps <p>802.11a Patch Antenna:</p> <ul style="list-style-type: none"> • Indoor: <ul style="list-style-type: none"> – 70 ft (21m) @ 54 Mbps – 150 ft (45m) @ 18 Mbps – 200 ft (61m) @ 6 Mbps • Outdoor: <ul style="list-style-type: none"> – 120 ft (36m) @ 54 Mbps – 700 ft (213m) @ 18 Mbps – 1200 ft (355m) @ 6 Mbps <p>802.11b Omni directional Antenna:</p> <ul style="list-style-type: none"> • Indoor: <ul style="list-style-type: none"> – 130 ft (40 m) @ 11 Mbps – 350 ft (107 m) @ 1 Mbps • Outdoor: <ul style="list-style-type: none"> – 800 ft (244 m) @ 11 Mbps – 2000 ft (610 m) @ 1 Mbps

Table 2 Product Specifications (Continued)

	With 802.11a radio installed	With 802.11b radio installed	With both 802.11a and 802.11b radio installed
Compliance	<ul style="list-style-type: none"> Standards: <ul style="list-style-type: none"> Safety: <ul style="list-style-type: none"> UL 1950 CSA 22.2 No. 950-95 IEC 60950 EN 60950 Radio Approvals: <ul style="list-style-type: none"> FCC Part 15.401-15.407 RSS-210 (Canada) EN 301.893 (Europe) ARIB STD-T71 (Japan) AS 4268.2 (Australia) EMI and Susceptibility (Class B): <ul style="list-style-type: none"> FCC Part 15.107 and 15.109 ICES-003 (Canada) VCCI (Japan) EN 301.489-1 and -17 (Europe) Other: <ul style="list-style-type: none"> IEEE 802.11a FCC Bulletin OET-65C RSS-102 	<ul style="list-style-type: none"> Standards: <ul style="list-style-type: none"> Safety: <ul style="list-style-type: none"> UL 1950 CSA 22.2 No. 950-95 IEC 60950 EN 60950 Radio Approvals: <ul style="list-style-type: none"> FCC Part 15.247 RSS-139-1, RSS-210 (Canada) EN 300.328 (Europe) Telec 33B (Japan) AS/NZS 3548 (Australia and New Zealand) EMI and Susceptibility (Class B): <ul style="list-style-type: none"> FCC Part 15.107 and 15.109 ICES-003 (Canada) VCCI (Japan) EN 301.489-1 and -17 (Europe) Other: <ul style="list-style-type: none"> IEEE 802.11b FCC Bulletin OET-65C RSS-102 	<ul style="list-style-type: none"> Standards: <ul style="list-style-type: none"> Safety: <ul style="list-style-type: none"> UL 1950 CSA 22.2 No. 950-95 IEC 60950 EN 60950 Radio Approvals: <ul style="list-style-type: none"> FCC Part 15.401-15.407 RSS-210 (Canada) EN 301.893 (Europe) ARIB STD-T71 (Japan) AS 4268.2 (Australia) FCC Part 15.247 RSS-139-1, RSS-210 (Canada) EN 300.328 (Europe) Telec 33B (Japan) AS/NZS 3548 (Australia and New Zealand) EMI and Susceptibility (Class B): <ul style="list-style-type: none"> FCC Part 15.107 and 15.109 ICES-003 (Canada) VCCI (Japan) EN 301.489-1 and -17 (Europe) Other: <ul style="list-style-type: none"> IEEE 802.11a IEEE 802.11b FCC Bulletin OET-65C RSS-102
SNMP compliance	<ul style="list-style-type: none"> MIB¹ I and MIB II 	<ul style="list-style-type: none"> MIB I and MIB II 	<ul style="list-style-type: none"> MIB I and MIB II
Antenna	<ul style="list-style-type: none"> Integrated 6 dBi diversity patch (55 degree horizontal, 55 degree vertical beamwidths, 5 dBi diversity omnidirectional with 360 degree horizontal and 40 degree vertical beamwidths) 	<ul style="list-style-type: none"> Two RP-TNC connectors (antennas optional, none supplied with unit) 	5 GHz: <ul style="list-style-type: none"> Integrated 6 dBi diversity patch (55 degree horizontal, 55 degree vertical beamwidths, 5 dBi diversity omnidirectional with 360 degree horizontal and 40 degree vertical beamwidths) 2.4 GHz: <ul style="list-style-type: none"> Two RP-TNC connectors (antennas optional, none supplied with unit)

Table 2 Product Specifications (Continued)

	With 802.11a radio installed	With 802.11b radio installed	With both 802.11a and 802.11b radio installed
Security architecture client authentication	<ul style="list-style-type: none"> • 802.1X support, including LEAP and EAP-TLS, to yield mutual authentication and dynamic, per-user, per-session WEP² keys • Authentication by MAC³ address and by standard 802.11 authentication mechanisms • Encryption: Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits; support for WEP enhancements such as key hashing (per-packet keying) and MIC 	<ul style="list-style-type: none"> • 802.1X support, including LEAP and EAP-TLS, to yield mutual authentication and dynamic, per-user, per-session WEP keys • Authentication by MAC address and by standard 802.11 authentication mechanisms • Encryption: Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits; support for WEP enhancements such as key hashing (per-packet keying) and MIC 	<ul style="list-style-type: none"> • 802.1X support, including LEAP and EAP-TLS, to yield mutual authentication and dynamic, per-user, per-session WEP keys • Authentication by MAC address and by standard 802.11 authentication mechanisms • Encryption: Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits; support for WEP enhancements such as key hashing (per-packet keying) and MIC
Status LEDs	<ul style="list-style-type: none"> • Three indicators on the top panel report association status, operation, error/warning, firmware upgrade, and configuration, network/modem, and radio status. 	<ul style="list-style-type: none"> • Three indicators on the top panel report association status, operation, error/warning, firmware upgrade, and configuration, network/modem, and radio status. 	<ul style="list-style-type: none"> • Three indicators on the top panel report association status, operation, error/warning, firmware upgrade, and configuration, network/modem, and radio status.
Software Image Network and Inventory support	<ul style="list-style-type: none"> • CiscoWorks RME⁴, CiscoWorks SWIM⁵ 	<ul style="list-style-type: none"> • CiscoWorks RME, CiscoWorks SWIM 	<ul style="list-style-type: none"> • CiscoWorks RME, CiscoWorks SWIM
Remote configuration support	<ul style="list-style-type: none"> • BOOTP, DHCP⁶, Telnet, HTTP, FTP⁷, TFTP⁸, and SNMP 	<ul style="list-style-type: none"> • BOOTP, DHCP, Telnet, HTTP, FTP, TFTP, and SNMP 	<ul style="list-style-type: none"> • BOOTP, DHCP, Telnet, HTTP, FTP, TFTP, and SNMP
Local configuration	<ul style="list-style-type: none"> • Direct console port (RJ-45 interface) 	<ul style="list-style-type: none"> • Direct console port (RJ-45 interface) 	<ul style="list-style-type: none"> • Direct console port (RJ-45 interface)
Dimensions	<ul style="list-style-type: none"> • 6.562 in. (16.67 cm) wide; 7.232 in. (18.37 cm) deep; 1.660 in. (4.22 cm) high • Mounting bracket adds 0.517 in. (1.31 cm) to the height 	<ul style="list-style-type: none"> • 6.562 in. (16.67 cm) wide; 7.232 in. (18.37 cm) deep; 1.660 in. (4.22 cm) high • Mounting bracket adds 0.517 in. (1.31 cm) to the height 	<ul style="list-style-type: none"> • 6.562 in. (16.67 cm) wide; 7.232 in. (18.37 cm) deep; 1.660 in. (4.22 cm) high • Mounting bracket adds 0.517 in. (1.31 cm) to the height
Weight	<ul style="list-style-type: none"> • 26 oz (737g) add 6.4 oz (181g) for mounting bracket 	<ul style="list-style-type: none"> • 25.6 oz (724g) add 6.4 oz (181g) for mounting bracket 	<ul style="list-style-type: none"> • 27.6 oz (783g) add 6.4 oz (181g) for mounting bracket
Environmental	<ul style="list-style-type: none"> • -4° to 122°F (-20° to 50°C), 10 to 90% humidity (noncondensing) 	<ul style="list-style-type: none"> • -4° to 131°F (-20° to 55°C), 10 to 90% humidity (noncondensing) 	<ul style="list-style-type: none"> • -4° to 122°F (-20° to 50°C), 10 to 90% humidity (noncondensing)
Processor	<ul style="list-style-type: none"> • IBM PowerPC405 200 MHz 	<ul style="list-style-type: none"> • IBM PowerPC405 200 MHz 	<ul style="list-style-type: none"> • IBM PowerPC405 200 MHz
System Memory	<ul style="list-style-type: none"> • 16 Mbytes RAM • 8 Mbytes FLASH 	<ul style="list-style-type: none"> • 16 Mbytes RAM • 8 Mbytes FLASH 	<ul style="list-style-type: none"> • 16 Mbytes RAM • 8 Mbytes FLASH
Input power requirements	<ul style="list-style-type: none"> • 90 to 240 VAC +/- 10% (power supply) • 48 VDC +/- 10%(device) 	<ul style="list-style-type: none"> • 90 to 240 VAC +/- 10% (power supply) • 48 VDC +/- 10%(device) 	<ul style="list-style-type: none"> • 90 to 240 VAC +/- 10% (power supply) • 48 VDC +/- 10%(device)

Table 2 Product Specifications (Continued)

	With 802.11a radio installed	With 802.11b radio installed	With both 802.11a and 802.11b radio installed
Power Draw	<ul style="list-style-type: none"> • 8 watts, RMS 	<ul style="list-style-type: none"> • 6 watts, RMS 	<ul style="list-style-type: none"> • 11 watts, RMS
Warranty	<ul style="list-style-type: none"> • One year 	<ul style="list-style-type: none"> • One year 	<ul style="list-style-type: none"> • One year

1. Management Information Base

2. Wired Equivalent Privacy

3. Media Access Control

4. CiscoWorks Resource Manager Essentials

5. Software Image Manager

6. Dynamic Host Configuration Protocol

7. File Transfer Protocol

8. Trivial File Transfer Protocol

Table 3 Product System Requirements

Feature	System requirement
Standard 802.1X-compliant user-level authentication and dynamic encryption keying	One of the following RADIUS servers: <ul style="list-style-type: none">• Cisco Secure Access Control Server Version 3.0 or greater• Cisco Access Registrar Version 1.7 or greater• Funk Software Steel Belted RADIUS Server Version 3.0 or greater• Interlink Networks RAD-Series RADIUS Server Version 5.1 or greater
CiscoWorks RME/SWIM	• CiscoWorks LMS ¹ or RWAN ²
Line power over Ethernet support (2.4 GHz radio only)	<ul style="list-style-type: none">• Cisco AIR-PSINJSYS1200= single-port power injector• Cisco Catalyst® 3524-PWR XL Switch• Cisco Catalyst 4006 and 6500 Series switches with inline power• Cisco WS-PWR-PANEL Midspan Power Patch Panel
Line power over Ethernet support (both 5 GHz and 2.4 GHz radio)	• Cisco AIR-PSINJSYS1200= single-port power injector
Line power over Ethernet support (5 GHz radio only)	• Cisco AIR-PSINJSYS1200= single-port power injector

1. LAN Management Solution

2. Routed WAN Management Solution

APPENDIX B ORINOCO 802.11A/B COMBO SPECIFICATIONS

ORINOCO 802.11a/b ComboCard Specifications		
INTERFACE		
CardBus Card (32-bit) Type II PC Card		
RADIO CHARACTERISTICS		
802.11a		
Frequency Bands	5150-5250; 5250-5350; 5725-5825 MHz	
Modulation Technique	64 QAM, 16 QAM, QPSK, BPSK	
Media Access Protocol	CSMA/CA (Collision Avoidance) with ACK	
Nominal Output Power	17 dBm	
Power Consumption PC Card	Doze mode – 15 mA Receive – 320 mA Transmit – 560 mA	
Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps per channel, auto fallback for extended range Proxim 20™ Mode: 108, 96, 72, 48, 36, 24, 18, 12 Mbps per two (2) channels, auto fallback for extended range	
802.11b		
Frequency Bands	2400 - 2484 MHz	
Modulation Technique	Direct Sequence Spread Spectrum (DSSS, DQPSK, DBPSK)	
Media Access Protocol	CSMA/CA (Collision Avoidance) with ACK	
Nominal Output Power	18 dBm	
Power Consumption PC Card	Doze mode – 15 mA Receive – 341 mA Transmit – 576 mA	
Data Rates	11, 5.5, 2, 1 Mbps per channel, auto fallback for extended range	
PHYSICAL SPECIFICATIONS		
Dimensions	117.8 mm X 53.95 mm X 5 mm (PC Card)	
Weight	55 gram	
ENVIRONMENTAL SPECIFICATIONS		
	Temperature	Humidity
Operating	0 to 70°C	95% (non condensing)
Storage	-65 to 150°C	95% (non condensing)
PC CARD SPECIFICATIONS		
Type II CardBus	32-bit interface	
Power Supply Voltage	3.3VDC from host (+/-0.2V)	
LEDs		
2 LEDs:	Power Network Activity	
SECURITY		
Gold	802.1x with support for EAP – TLS, EAP – TTLS and EAP – MD5	
Silver & Gold	AES: 128/128/64-bit WEP for 802.11a, 128/64-bit WEP for 802.11b	
WARRANTY		
3 years		
PACKAGE CONTENTS		
• CardBus Card • Getting Started Guide • CD-ROM with drivers, installation and configuration utility, Boingo software and user's guide.		
ORDERING INFORMATION		
8460	ORINOCO Gold 802.11a/b ComboCard	
8461	ORINOCO Silver 802.11a/b ComboCard	

Figure 14. Orinoco 802.11a/b Combo Specifications
(From: www.orinocowireless.com, Jan 03)

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C SECURITY GUIDELINES FOR WIRELESS LAN

The following are some of the guidelines that could help to reduce the exposure of a network to the wireless LAN security threats:

Access Point Physical Security

The access points should be properly secured within the office environment to prevent them from any unauthorized access and physical tampering. These access points should be placed in a well accessible location to allow easy security setting and maintenances especially if the company has a few hundreds of these access points to support.

To avoid interferences to its services, these access points should be physically located away from external sources of electromagnetic interference, e.g. microwave ovens. In additional, they should be waterproof for external installation.

Information Confidentiality and Integrity

The IEEE 802.11b standard allows for an optional privacy facility known as Wired Equivalent Privacy (WEP). The technique uses shared keys and a pseudo random number (PRN) as an initial vector (IV) to encrypt the data portion of network packets. This is based on the use of secret keys with symmetric encryption algorithms. The 802.11b wireless LAN network headers (including the IV portion and key number) themselves are not encrypted. This is one of the vulnerability, which an attacker could exploit. Although the standard specifies support for the popular RC4 symmetric stream cipher, all new symmetric key encryption efforts should be based on the AES block cipher in Offset Codebook Mode. The OCB has been optimized to minimize the number of calls to lower level cryptographic primitives, and can both encrypt/decrypt and tag/verify a message in a single pass.

With the recent discoveries of the WEP vulnerability, the WEP encryption should not be used as the only form of protection. Confidential or important information should be encrypted prior to transmission over the wireless LAN so as to protect its confidentiality and integrity. In additional, cryptographic hashing function such as MD-5

or SHA-1 can also be used to ensure the integrity of the information transmitted over the wireless LAN.

Wireless LAN Key Management

The symmetric encryption keys, e.g. the WEP keys stored in the access points and wireless station, should be protected from unauthorized access. The unauthorized intruder could use the encryption keys to decipher the wireless LAN data traffic. When in operation, the default WEP encryption keys should be changes and these keys should be changed on daily to weekly basics.

While existing wireless LAN products support WEP services using 40- or 64-bits keys, newer one can support the use of longer and more secure 128-bit keys. However, the longer keys may impact the overall performance of the wireless LAN.

The symmetric encryption keys should be protected during the key distribution to the users. The new keys should be send to the users either in encrypted form or through other secure means to prevent unauthorized access to the keys.

Instead on relying on the shared static symmetric base key, a session key tie to a particular session could be generated for the symmetric encryption. The advantages for these arrangements are:

- To prevent the shared static symmetric base key from direct attack
- Each party accessing the wireless LAN has its own set of encryption key.

However, the session keys are still subject to spoofing if the base key is revealed to an intruder.

User Authentication Mechanism

Currently, only the Service Set Identifiers (SSID) and MAC address are the access control mechanisms supported by the wireless LAN technology, only verify authorized wireless stations but not the users. As such, unauthorized personnel can gain access to the wireless LAN and its network resources using a stolen wireless station.

To authenticate the identity of the users accessing the wireless LAN, user authentication mechanisms such as users' ids/passwords, smart cards, security token (e.g.

RSA SecurID two-factor authenticator) should be used to stop unauthorized access to the company's internal network via the wireless LAN.

Access Control

In addition to the above SSID and MAC access control mechanism, which are built into the IEEE 802.11 wireless LAN standard, the following mechanisms should be employed to further enhance the security of a wireless LAN:

Wireless Network Access ID. Most wireless LAN products allow the configuration of a user-defined access ID that can be used to further restrict access of the radio adaptors to the specific access points. Only when the access ID is the same can the adapter connect to that access point and join the cell. However, every access point and adapter can only use one network ID. This is unlike WEP, which allows every access point and adapter to be configured to use different secret keys for different transmissions.

Ethernet/MAC Address Restriction. Every Ethernet adapter has a unique universal 12-digit hexadecimal MAC address and the wireless adapter has one too. This IEEE-controlled hardware address can be used to identify the wireless client on the network. We can make use of this "feature" by configuring each access point to only accept connections from adapters with registered MAC addresses. This provides a certain degree of security against unauthorized access. However, MAC addresses can still be spoofed, so this should not be used on its own but in combination with the other mechanisms to further reduce the likelihood of unauthorized access to the wireless LAN.

Network Authentication. A good network operating system, such as Novell, Windows NT/2000, minimally requires the user to log on by supplying a correct user ID and password before he can gain access to the network. Wireless LAN users should be required to do the same.

Firewall Access Control. Access control mechanisms such as firewalls should be implemented to segregate the wireless LAN from the internal wired network. The wireless LAN should be deployed in a different network segment, which is separate from the internal wired network. Network or IP filtering can be implemented at the gateway to ensure that only authorized network traffic from the wireless LAN or legitimate access

points are allowed to enter the wired network. This is to prevent unauthorized access to the internal wired network via rogue access points.

Figure 15 shows how a firewall is used to segregate the wireless LAN from the internal wired network

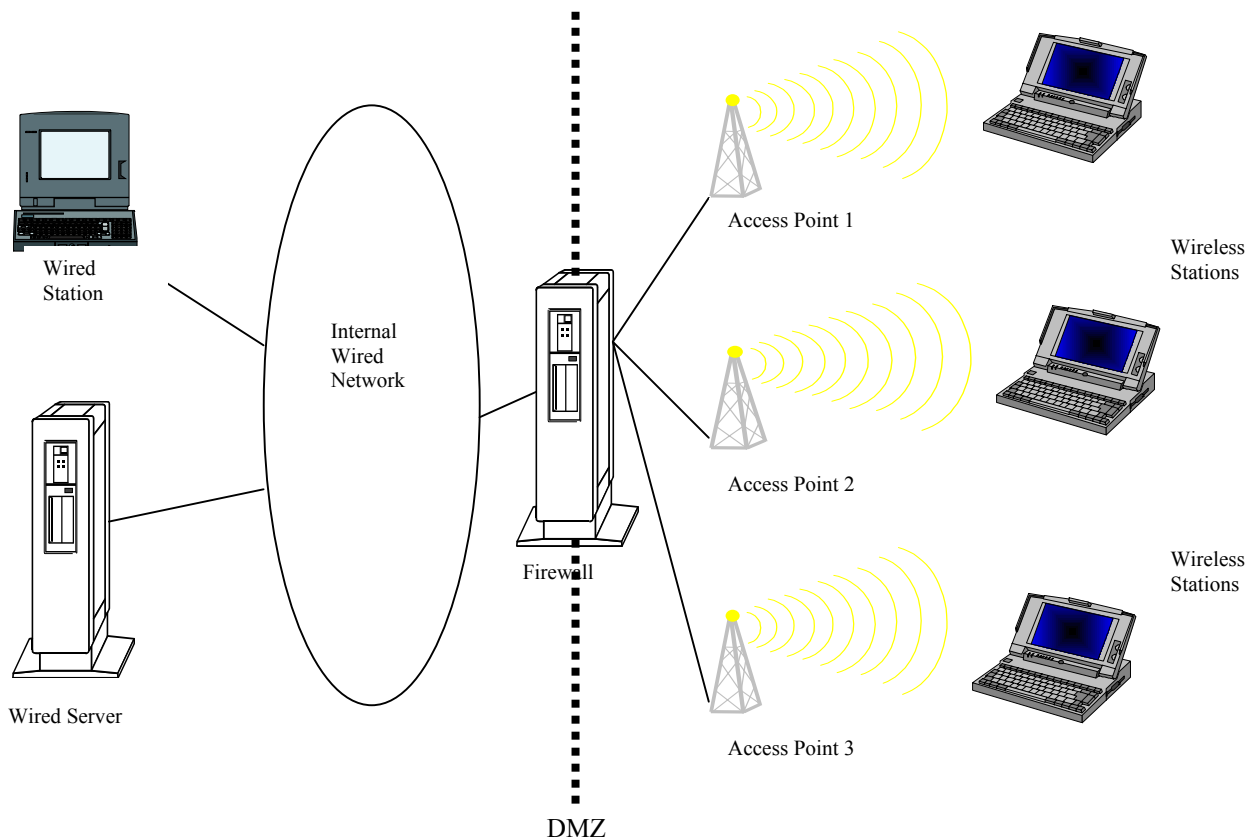


Figure 15. Use of Firewall to Segregate Wireless LAN from Wired Network

Wireless Station Security

On the client wireless station, access control and intrusion detection mechanisms should be installed where possible to prevent and detect any unauthorized access over the wireless LAN. The attacker may compromise on the client station and uses it to access the internal wired network.

The user's privileges and access rights to the systems and network resources should be restricted if they access the wireless LAN using client computing devices where there are no controls available, e.g. PDAs.

Software programs that can be used to configure the wireless station as access point should not be allowed so as to minimize the set-up of rogue access points. This is to prevent unauthorized access to the internal wired network via the rogue access point due to insecure configurations (e.g. WEP not enabled, no MAC address control list).

An access point authenticates a user, but a user does not and cannot authenticate an access point. If a rogue access point is placed on a wireless LAN, it can be a launch pad for denial-of-service attacks through the “hijacking” of the wireless station of legitimate users. Mutual authentication supported by the access point allows the mutual authentication between the client and the authentication server, where both sides prove their legitimacy. Mutual authentication also makes it possible to detect and isolate rogue access points.

The wireless station should also not be configured for network file sharing without any protection to prevent any unauthorized access to his local files.

User Security Awareness

Users within the company premise should not be allowed to set up their wireless stations in ad-hoc mode and communicate with each other without going through the access point. This is to prevent unauthorized access to the user’s files if they are not protected.

The user should power down the wireless station when it is not being used for a long period of time, e.g. after office hours. This will reduce the risk of attacks on the wireless station over the wireless LAN. When the user’s wireless station has made connected to the internal wired network, it should not have concurrent direct connection to any untrusted network, e.g. the Internet. This is to prevent any unauthorized access to the internal wired network via the wireless station.

Access Points Administration and Maintenance

Only administrators have access to the wireless LAN key distribution program for the distribution of the encryption keys. The built-in COM ports of the access point should be disabled or password-protected to prevent any unauthorized access to the access points. All unnecessary services and ports in the access points should be removed or closed.

Periodic scanning on the wireless LAN should be conducted to detect the presence of rogue access points, unauthorized ports/services or any security vulnerabilities in the network. Prior to the scanning process, written approval should be obtained from the management to allow the vulnerabilities scanning on the network.

The password for remote management of access points can be captured and used to gain unauthorized access to the access points. As such, administration of access points should not be done over the wireless LAN. Instead, the access points should be administrated via the wired network or locally via the access point's built-in COM ports.

It is commonly to statically assign a WEP key to a client, either on the client's disk storage or in the memory of the client's wireless LAN adapter. When a wireless station is lost, the intended user of the wireless station no longer has access to the MAC address or WEP key, and an unintended user does. This should be reported immediately to the network administrator. This would allow prompt action to be taken to prevent any unauthorized access via the lost wireless equipment, e.g. render the MAC address and WEP key useless for wireless LAN access and decryption of transmitted data. The administrator must recode static encryption keys on all clients that use the same keys as the lost or stolen wireless station. As the number of clients increases, the task of reprogramming WEP keys becomes more taunting. To overcome this limitation is a security scheme that:

Bases wireless LAN authentication on device-independent items such as usernames and passwords, which users possess and use regardless of the wireless station on which they operate

Uses WEP keys that are generated dynamically upon user authentication, not static keys that are physically associated with a wireless station.

Logging and Audit

Logging of the wireless LAN helps to detect unauthorized network traffic, e.g. using Intrusion Detection System, to detect attacks directed over the wireless LAN. Logging information such as source/destination IP addresses, MAC addresses, user's logon names/ids and logon time/duration can be logged to aid analysis and investigation in the event of network problem. On periodical basics, audit should also be performed to

detect any exceptions or abnormal network activities and alert should be sent to the network administrators

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- [1] Stallings, William. *Wireless Communications and Networks*. Prentice Hall, 2002.
- [2] Douglas E. Comer, *Computer Networks and Internets*, Third Edition, Prentice Hall, 2001.
- [3] Wheat Jeffrey and others, *Designing A Wireless Network*, Syngress Publishing, Inc., 2002.
- [4] Cisco Aironet 1200 series Access Point, <http://www.cisco.com/>, Dec 2002.
- [5] Grier, Jim. *Minimizing WLAN Security Threats*. <http://www.wireless-nets.com/bio.htm>, 2003.
- [6] <http://intranet.nps.navy.mil/wireless/>, Jan 2003
- [7] http://www.atheros.com/pt/atheros_wlansecurity.pdf, Feb 2003.
- [8] IEEE Std 802.11i/D3.0, Nov 2002

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Chair, IS Department
Naval Postgraduate School
Monterey, California
4. Professor Norman Schneidewind
Naval Postgraduate School
Monterey, California
5. Professor Douglas Brinkley
Naval Postgraduate School
Monterey, California
6. Lieutenant Colonel Tay Chye Bin
Ministry of Defense, Singapore